

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 2004 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

5990-8809
March, 2004
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	ix
Chapter 1	Introduction	1-1
	700wl Series Overview	1-1
	700wl Series Functions	1-3
	Client Authentication	1-3
	Client Access Rights	1-4
	Wireless Data Privacy and VPN Protocols	1-4
	Roaming Support	1-4
	Network Address Translation	1-5
	VLAN Tag Support	1-6
Chapter 2	Using the 700wl Series System	2-1
	Initial Configuration of the 700wl Series System	2-1
	Managing and Administering the 700wl Series System	2-2
	Centralized Administration	2-3
	Logging on to the Administrative Console	2-4
	Changing the Built-In Administrator Username and Password	2-5
	Using Online Help	2-5
	Logging Out	2-6
	Using the Administrative Console	2-7
	Header Bar and Navigation Bar	2-7
	Tabs	2-10
	Basic System Configuration Tasks	2-16
	Setting Up Authentication and Access Rights	2-16
	System Features and Concepts	2-17
	Centralized Management and Administration	2-17
	Enterprise Class Redundancy	2-18
	Bandwidth Management	2-20
	Addressing in the 700wl Series System	2-21
	Layer 3 Roaming Support	2-23
	VLANs and the 700wl Series System	2-24

Chapter 3	System Status	3-1
	Viewing Status Information	3-1
	Viewing Equipment Status	3-3
	Viewing Access Control Server Status	3-4
	Viewing Access Controller Status	3-5
	Viewing Access Controller Status Details	3-5
	Viewing Client Status	3-7
	Filtering Client Status Information	3-9
	Viewing Client Details	3-9
	Viewing Session Status	3-12
	Filtering Session Status Information	3-14
	Viewing License Information	3-15
Chapter 4	Configuring Rights	4-1
	Access Rights in the 700wl Series System	4-1
	The Rights Manager	4-4
	Configuring Access Rights—An Overview	4-5
	The Rights Assignment Table	4-6
	Adding or Editing a Rights Assignment	4-9
	Identity Profiles	4-11
	Creating or Editing an Identity Profile	4-13
	Users in the Built-In Database	4-16
	Creating or Editing a User	4-17
	Network Equipment in the Built-in Database	4-20
	Creating or Editing an Equipment Entry	4-22
	Retrieving MAC Addresses from an LDAP Database	4-24
	Specifying an LDAP Service for MAC Address Retrieval	4-25
	Configuring the Search for MAC Addresses	4-26
	Connection Profiles	4-29
	Creating or Editing a Connection Profile	4-31
	Locations	4-35
	Time Windows	4-37
	Access Policies	4-39
	Viewing Filters—the Grid Views	4-41
	Creating or Editing an Access Policy	4-43
	Allowed Traffic Filters	4-62
	Redirected Traffic Filters	4-66
	DNS/WINS Filter Pairs	4-72
	HTTP Proxy Filters	4-75
	Example—Modifying the “Guest Access” Access Policy	4-79
	Enabling an Existing Allowed Traffic Filter—Outside World	4-79

	Modifying the Outside World Filter to Restrict Access	4-82
	Setting Up HTTP Proxy Filters	4-83
Chapter 5	Configuring Authentication	5-1
	Authentication in the 700wl Series System	5-1
	The Rights Manager	5-4
	Authentication Policies	5-4
	Creating or Editing an Authentication Policy	5-6
	Configuring Authentication Services	5-7
	Configuring an LDAP Authentication Service	5-8
	Using the Active Directory LDAP Service	5-13
	Using a Netscape or iPlanet Directory Service	5-14
	Configuring the 802.1X Authentication Service	5-16
	Configuring a Kerberos Authentication Service	5-17
	Configuring a RADIUS Authentication Service	5-19
	Using RADIUS for Accounting	5-20
	Configuring an XML-RPC Authentication Service	5-22
	NT Domain Logon	5-27
	External Identity Retrieval	5-28
	Logon Page Customization	5-30
	Customizing a Logon Page	5-32
	Customizing the Stop Page	5-37
	Customized Page Templates	5-39
	Tools and Options	5-42
	Simulating User Rights	5-42
	Tracing Authentication Service Transactions	5-47
	Importing and Exporting the Rights Configuration	5-49
Chapter 6	Configuring the Network	6-1
	700wl Series System Components	6-2
	The System Components List	6-2
	Configuring an Access Control Server	6-3
	Configuring an Integrated Access Manager	6-7
	Configuring Access Controllers	6-10
	Organizing Access Controllers into Folders	6-13
	Configuring Failover with Redundant Access Control Servers	6-15
	The Secondary Access Control Server	6-16
	Disabling Redundancy	6-17
	Configuring Network Communication—Network Setup	6-17
	Network Communication—the Basic Setup Tab	6-19
	Advanced Network Configuration—the Advanced Setup Tab	6-21
	Automatic HTTP Proxy Server Specification	6-26

	SSL Certificate	6-28
	Configuring Network Interfaces	6-34
	Configuring the Port Speed and Duplex Settings	6-34
	Port Subnet IP Address and Subnet Netmask	6-36
	Configuring SNMP	6-38
	Setting the Date and Time	6-40
	Setting Up Administrators	6-42
	Editing an Administrator's Settings	6-44
	Editing Your Administrator Password	6-45
Chapter 7	Setting up Wireless Data Privacy	7-1
	Overview of Wireless Data Privacy	7-1
	Wireless Data Privacy Setup	7-2
	Global Wireless Data Privacy Configuration	7-3
	Configuration for IPSec	7-3
	IPSec Certificate Configuration	7-5
	IP Address Assignment for Tunneling	7-11
	VPN Tunneling and Network Address Translation	7-12
Chapter 8	System Maintenance	8-1
	Software Setup	8-1
	Updating the System Software	8-2
	Remote Update	8-5
	Local Update	8-9
	Restarting Using the Alternate Version Software	8-12
	Backing Up and Restoring the System Configuration	8-13
	Creating the Backup Image	8-14
	Saving the Backup as a File	8-15
	Restoring From a Backup File	8-16
	Transferring a Backup to a Different System	8-17
	Shutting Down and Restarting a System Component	8-18
	Restarting a System Component	8-19
	Shutting Down a System Component	8-20
	Resetting to Factory Default Settings	8-21
Chapter 9	Logs	9-1
	Viewing 700wl Series System Logs	9-1
	Configuring Session Logging	9-4
	Viewing the Session Logs	9-6
	The Session Log Entry Format	9-6

Appendix A	Command Line Interface	A-1
	Accessing the Command Line Interface	A-2
	Connecting with a Serial Console	A-2
	Connecting Using SSH	A-2
	Using the CLI on an Integrated Access Manager	A-2
	Command Syntax	A-3
	Getting CLI Command Help	A-3
	Administrator Access Control Commands	A-4
	System Status and Information Commands	A-6
	Network Configuration Commands	A-9
	Port Configuration Commands	A-12
	Access Controller Port Status Commands	A-13
	Access Controller Configuration	A-14
	Advanced Network Configuration Status	A-15
	Access Control Server Configuration	A-15
	Advanced Network Configuration	A-18
	Remote Commands	A-18
	Wireless Data Privacy Configuration	A-21
	Active Client Management Commands	A-23
	System Backup, Upgrade and Shutdown Commands	A-25
	Backup and Restore	A-25
	Upgrading the System Software	A-27
	Stopping and Restarting the System	A-29
	Resetting to Factory Defaults	A-30
	Diagnostic and Log Commands	A-30
	Time Configuration	A-33
	SNMP Configuration and Reporting Commands	A-34
Appendix B	Filter Expression Syntax	B-1
	Introduction	B-1
	Filter Specification Syntax	B-1
	Tcpdump Primitives	B-2
Appendix C	Creating Customized Templates	C-1
	Introduction	C-1
	A Simple Logon Page Template Example	C-2
	Example 1	C-2
	Logon Template Elements	C-3
	Required Elements	C-4

Optional Elements	C-5
Logon Page Template — A More Advanced Example	C-7
Example 2	C-7
Changing the Logon Button Names	C-10
Example 3	C11
Customizing the Logon Page Messages	C-12
Guest Registration Template	C-13
Example 4	C-14
Using a Logoff Pop-Up with a Customized Logon Page	C-16
Example 5	C-17
Redisplaying the Logon Page in a New Window	C-18
Customizing the Stop Page	C-19
Appendix D Troubleshooting	D-1
Appendix E Glossary	E-1
Index of Commands	IOC-1
Index	IX-1

PREFACE

This preface describes the audience, use, and organization of the *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 system. 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 Integrated Access Manager, Access Control Server, and Access Controller. 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 Tahoma	Screen menus, commands, or field names that you select are in boldface Arial.
<i>Boldface Italic Palatino</i>	New terms that are introduced are in boldface italic Palatino.
<i>Italic Palatino</i>	Emphasized terms and cross references to other areas in the manual 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 of special importance in certain situations.
None	Caution	Risk of system functionality loss or data loss.
	Warning	Risk of personal injury, system damage, or irrecoverable data loss.

Document Organization

This manual is organized as follows:

Chapter 1—Introduction

This chapter provides an introduction to the 700wl Series system.

Chapter 2—Using the 700wl Series System

This chapter helps you get started using the 700wl Series system and its Administrative Console. It gives an overview of what you can do and provides pointers to where to learn more for each task and procedure.

Chapter 3—System Status

This chapter describes the status component of the 700wl Series system. It explains how to monitor equipment, client, and session status.

Chapter 4—Configuring Rights

This chapter describes how network access rights are assigned to clients through the 700wl Series system, and explains how to configure access control policies.

Chapter 5—Configuring Authentication

This chapter describes how clients are authenticated through the 700wl Series system, and explains how to configure authentication policies.

Chapter 6—*Configuring the Network*

This chapter describes how to configure the 700wl Series system components so that they work with your enterprise network.

Chapter 7—*Setting up Wireless Data Privacy*

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

Chapter 8—*System Maintenance*

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

Chapter 9—*Logs*

This chapter explains how to configure, examine and use the 700wl Series system log.

Appendices

Appendix A—*Command Line Interface*

This appendix provides a description of the 700wl Series system command line interface.

Appendix B—*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 C—*Creating Customized Templates*

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

Appendix D—*Troubleshooting*

This appendix presents troubleshooting procedures for the 700wl Series system, including the symptoms, probable cause and recommended actions for a variety of problems.

Appendix E—*Glossary*

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

Index of Commands

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

Related Publications

There are several other publications related to the 700wl Series that may be useful:

- *700wl Series Software Release Notes* provides the most up-to-date information on the current software release.
- The *700wl Series Installation and Getting Started Guide* documents the initial system installation and configuration of your HP ProCurve hardware unit.
- The *700wl Series Quick Start Guide* provides a much briefer overview of the system installation of your hardware unit.
- The *700wl Series Wireless Data Privacy™ Guide* provides information and instructions for configuring Wireless Data Privacy on the 700wl Series system, including information and instructions on configuring selected Wireless Data Privacy clients on Windows and Macintosh client systems.
- The *700wl Series Software Migration Guide* provides important information and instructions for customers who are upgrading from 700wl Series system software version 3.0 or 3.1 to version 4.0 or later.

All system documentation is available on the HP ProCurve Technical Support web site at <http://www.hp.com/rnd/index.htm>. In addition, all documentation except the Release Notes is available on the 700wl Series Documentation CD-ROM which accompanies each 700wl Series system unit.

INTRODUCTION

This chapter provides a brief introduction to the 700wl Series system™ and its primary features. The topics covered in this chapter include:

700wl Series Overview	1-1
700wl Series Functions	1-3

700wl Series Overview

The 700wl Series system's industry-leading cost-performance and uniquely flexible and scalable deployment architecture provides the foundation for a secure, scalable, mission-critical 802.11 wireless network. At the core of the wireless LAN (WLAN) the 700wl Series system provides key services including centralized management and control, role-based fine-grained access policy enforcement, secure Layer 3 roaming, and tiered layers of security, which enables companies to deploy and manage 802.11 networks ranging from tens to thousands of access points (APs).

A 700wl Series system consists of a central Access Control Server 740wl that provides services such as authentication, roaming, and policy management, and one or more Access Controller 720wl units. Access Controllers are gateway devices deployed at the edge of the network in the user data path enforcing network authorization and business policy.

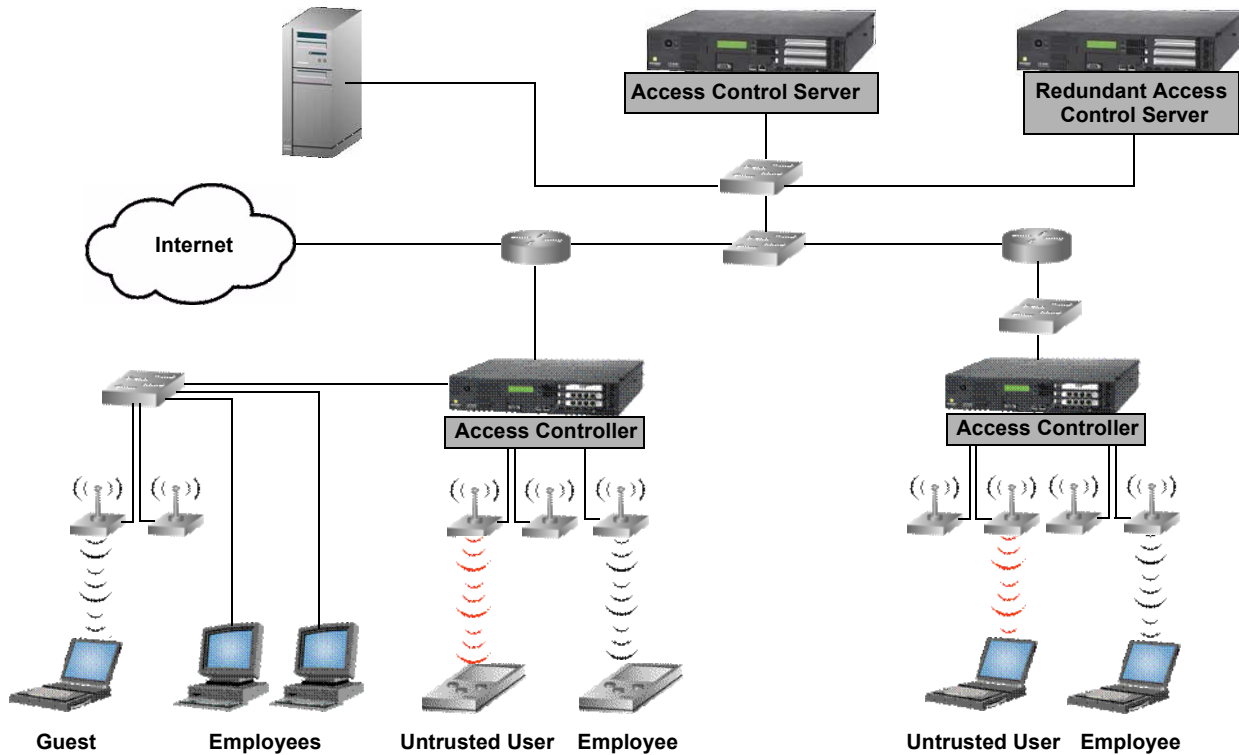
The *Access Controller* (the HP ProCurve Access Controller 720wl) is a low cost, high-performance appliance with modular connectivity options that require minimal configuration, and are deployed in conjunction with an HP ProCurve Access Control Server 740wl. The Access Controller sits between the Wireless Access Points and the network, and implements a powerful Packet Inspection Engine (Layer 2-7) that can rewrite and redirect client traffic based on an Access Policy received from the Access Control Server. Each Access Policy is tailored to the individual client based on who the client is (per a successful authentication) and where and when the client has connected to the network.

The *Access Control Server* (the HP ProCurve Access Control Server 740wl) is a centralized resource on the network that provides services to the connected Access Controllers such as authentication management, mobility management (roaming support), policy management, and system monitoring and reporting. The Access Control Server is deployed as a dedicated control function and does not sit in the user data path. A second Access Control Server can be deployed in a redundant configuration to support stateful failover.

Introduction

Figure 1-1 illustrates a 700w1 Series system topology that is configured with redundant Access Control Servers for failover.

Figure 1-1. 700w1 Series topology



Access Controllers sit at or near the edge of the network, and enforce authentication and access policies. As shown in Figure 1-1, Access Points are typically connected directly to Access Controller ports, but it is also possible to connect APs or clients through devices such as switches or hubs. When a client is detected at an Access Controller port, the Access Controller must first determine *who* the client is based on the Authentication Policy in force for that port at that time of day. The 700w1 Series system supports a variety of authentication methods, and can interface with an organization's existing authentication services (such as an LDAP service, RADIUS, Kerberos, 802.1x or NT Domain Logon) or can handle authentication through its own built-in user database.

The Access Controller actually hands off the client authentication to the central Access Control Server, which manages the authentication process and returns the appropriate Access Policy to the Access Controller.

An Access Policy specifies the network addresses, services, and resources the client is permitted to access. The Access Policy can also specify that client traffic for certain destinations be redirected to alternate destinations. This capability is used by the 700w1 Series system to redirect traffic from an unknown client to a logon page. It can also be used to notify clients when they attempt to access non-permitted resources, or to redirect a request to a permitted resource. Traffic to a destination that is neither permitted nor redirected is dropped. An Access Policy may also specify other settings such as bandwidth limitations, HTTP Proxy Servers (including filtering to impose HTTP access control), and encryption requirements. Access Policies can be configured to "expire" after a specified length of time, or at a specific time, forcing the client to reauthenticate.

Clients that are successfully authenticated, Employees in Figure 1-1, are typically associated with Access Policies that provide access to secure network resources. Clients that are not successfully authenticated, Untrusted Users, are typically associated with an Access Policy that allows only the ability to logon. The 700wl Series system also provides a Guest logon feature and Access Policy, that can be used to provide limited network access to users designated as Guests, for example, Internet access via the network with no intranet access.

Access Policies are defined and maintained by the Access Control Server, but are administered by the Access Controller. Once a client has been identified and the appropriate Access Policy has been returned to the Access Controller, the Access Controller is responsible for filtering client traffic and either forwarding it to its destination, redirecting it to the appropriate alternate destination, or dropping it. The Access Control Server does not get involved again unless something occurs that requires a renewal of the client's rights, such as expiration of their existing rights, or roaming to a different location.

In addition to being the repository for the Authentication Policies, Access Policies, and other system configuration information, the Access Control Server maintains status for every Access Controller. This includes status for every client connected to the 700wl Series system and every client session.

700wl Series Functions

The 700wl Series system provides central control of Access Controllers, and clients. The key system functions are: client authentication, rights management, Wireless Data Privacy, roaming support, NAT, and VLANs.

Client Authentication

The 700wl Series system provides a great deal of flexibility in authenticating users. The system supports three types of authentication:

- **Browser-based logon:** With browser-based logon, the first time a client attempts an HTTP access, the Access Controller presents a browser-based logon page. After the user enters a logon ID and password, the Rights Manager authenticates the client 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.
- **VPN logon:** With VPN logon, the client initiates a connection to the network using L2TP or PPTP. The Access Controller 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 the HP 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 client has been successfully authenticated.

Once the client has been authenticated, rights for the client are requested from the Rights Manager.

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

The 700wl Series system supports the following authentication services, any of which can be used in an Authentication Policy:

- LDAP directory services, such as Active Directory or iPlanet LDAP server

Introduction

- 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.

User Authentication is discussed in detail in Chapter 5, *Configuring Authentication*.

Client Access Rights

At any given time a certain set of rights is in effect for each client attached to an Access Controller. These rights are based on a number of factors, including client authentication, client identity, location of the connection, VLAN tags, and the time and day. The Rights Manager manages the criteria for each client connection.

- The Rights Manager uses *Access Policies* to define what network resources a user can access at any given time. Access Policies are defined for a group, and an individual user's rights are determined by the groups to which he or she belongs.
- The Rights Manager uses *Identity Profiles* and *Connection Profiles* 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.
- A client is matched to an Identity Profile based on who they are. They are matched to a Connection Profile based on when and where they connect to the network. The Rights Manager uses the Identity Profile and Connection Profile to match the client with the appropriate Access Policy. This is done in the *Rights Assignment Table*.

Chapter 4, *Configuring Rights* describes this process in detail.

Wireless Data Privacy and VPN Protocols

The 700wl Series system's VPN component enables strong encryption of data between a client and the Access Controller. This provides additional security for data sent over the airwaves, replacing 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, tunnel mode 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 has been set up, clients can roam between access points and the 700wl Series system will maintain each session transparently to the client.

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. A *Linger Timeout* determines the length of time a client has to complete a roam, that is to appear at a new physical location after disappearing from the old physical location. The settings for timing out a roaming client are part of the client's assigned Access Policy; different clients can have different settings and one client can have different settings depending on their location, time of day, and so on.

If the client completes the roam within the linger time, no reconnect or authentication is needed—the client's connection state is maintained intact. If the client fails to complete the roam before the linger timer expires the 700wl Series system concludes the client has actually disconnected and logs the client off.

Roaming support is discussed in more detail in *VLANs and the 700wl Series System* in Chapter 2, *Using the 700wl Series System*.

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 addresses 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 uses this unique identifier for returned 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 to the nearest Access Controller while roaming, 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 an 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 the client. A client having an IP address not within the Access Controller's subnet 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, that is specifically 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 access points, and should be used with caution.

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

Addressing in the 700wl Series System in Chapter 2, and Chapter 4, *Configuring Rights* include more extensive discussions of addressing considerations and NAT.

VLAN Tag Support

The HP System provides support for Virtual LAN (VLAN) tagging in several ways:

- A client can be matched to a Connection Profile based on the VLAN ID (802.1Q tag) associated with the client traffic.
- The VLAN tag associated with the client traffic can be stripped, added, or rewritten before the traffic is forwarded onto the network, based on the Access Policy in force for the client.

Matching a client to a Connection Profile based on the VLAN tag effectively enables you to assign an Access Policy to clients in a specific VLAN. The Access Policies associated with the VLAN-specific Connection Profiles can be configured to modify the VLAN tagging of these clients, if necessary. By default, the tag associated with the client's traffic is removed so the client's traffic is sent on to the network untagged. This scenario can be useful if you want to use the client's VLAN membership only to assign access rights for the client, and once the Access Policy is in place, the VLAN tag is no longer used. Optionally you can configure the Access Policy to preserve the tag or you can replace the original tag with a different tag.

The 700wl Series system also provides limited support for assigning IP addresses through DHCP based on the VLAN tag of the incoming traffic. In the 700wl Series system, IP subnet ranges may be specified on a port-by-port basis. In order to restrict an IP range to members of a specific VLAN, you can associate a Connection Profile that filters for the desired VLAN with the port that defines the subnet range.

USING THE 700WL SERIES SYSTEM

This chapter provides a brief introduction to using the 700wl Series system and its Administrative Console. It also provides an overview and discussion of a number of common tasks you may need to accomplish. The topics covered in this chapter include:

Initial Configuration of the 700wl Series System	2-1
Managing and Administering the 700wl Series System	2-2
Logging on to the Administrative Console	2-4
Using the Administrative Console	2-7
Basic System Configuration Tasks	2-16
System Features and Concepts	2-17

This chapter assumes that you have installed your HP ProCurve Access Control Server or Integrated Access Manager as instructed in the *700wl Series Quick Start Guide* or the *700wl Series Installation and Getting Started Guide*. This chapter takes you through the next steps towards configuring and using the 700wl Series system. The first section takes you through the required settings from the “Complete the Configuration” steps in the *700wl Series System Quick Start Guide*.

This chapter assumes you are new to the 700wl Series system. For users who are upgrading their 700wl Series system from a previous software version to version 4.1, you should read the *700wl Series Introduction to Software Version 4.x*. The *Introduction to Software Version 4.x* document introduces you to software version 4.0 as part of the process of migrating your system, and explains what has changed from versions 3.0 and 3.1.

Initial Configuration of the 700wl Series System

The initial configuration of a 700wl Series system component, sufficient to allow network access, is described in both the *700wl Series Quick Start Guide* shipped with each hardware unit, and in more detail in the *700wl Series Installation and Getting Started Guide*.

If you have installed your 700wl Series system according to the instructions in the *Quick Start Guide*, it should be configured with a set of basic network configuration settings.

For an Access Control Server, these settings include:

- An IP address of the Access Control Server
- Subnet mask that defines the subnet associated with the Access Control Server (the default is 255.255.255.0 (/24))
- Name of the domain in which the 700wl Series system resides
- Default router (gateway) IP address

Using the 700wl Series System

- Primary and secondary DNS server addresses
- Shared secret, used to enable Access Controllers or a peer Access Control Server to establish a trusted communication relationship with the Access Control Server. This is actually an optional item in the initial installation process of an Access Control Server, but no system components will be able to communicate with the 700wl Series system until this is set, so it is recommended that you do it as part of the initial installation.

For an Access Controller, the initial settings include:

- IP address of the Access Controller
- Subnet mask that defines the subnet associated with the Access Controller (the default is 255.255.255.0 (/24))
- Domain name
- Default router (gateway) IP address
- Primary and secondary DNS server addresses
- IP address of the Access Control Server that will manage the Access Controller
- Shared secret of the Access Control Server

If you allow your 700wl Series system components to get their IP address from a DHCP server, the DHCP server can provide the domain, default router IP address, DNS addresses, and WINS addresses.

On a newly-installed or Factory Reset Access Control Server, the following defaults are in effect:

- The DHCP address range for use with NAT'ed clients is the 42.0.0.0 subnet
- An HP ProCurve-signed SSL certificate is in place
- SNMP is disabled
- Wireless Data Privacy settings (encryption protocols) are disabled
- The default Authentication Policy uses the built-in database for user authentication

Managing and Administering the 700wl Series System

A 700wl Series system consists of an HP ProCurve Access Control Server and one or more HP ProCurve Access Controllers, or an HP ProCurve Integrated Access Manager, optionally with additional Access Controllers connected. All the elements of your 700wl Series system are configured, monitored and managed centrally from the Access Control Server or Integrated Access Manager. This monitoring and management is done through the Administrative Console, a web-browser-based interface that runs on the Access Control Server or Integrated Access Manager.

Note: *An HP ProCurve Integrated Access Manager is effectively an Access Control Server and an Access Controller physically integrated into a single module. However, the 700wl Series system software internally handles the functions within an Integrated Access Manager as if they are two separate subsystems. Therefore, throughout this guide, system features are described in terms of Access Control Servers and Access Controllers. These features all apply to an Integrated Access Manager as well.*

The 700wl Series system provides three levels of administrator access:

- A *Network Administrator* can configure the network parameters that enable the 700wl Series system to function in a network, such as configuring IP addressing, interface configuration, date and time settings, SNMP access, and performing software updates and backups. The network administrator can perform these functions for all system components that make up a 700wl Series system. A Network Administrator cannot perform any functions under the Rights Manager, such as adding users, creating or modifying Access Policies, modifying the Rights Table, setting up Authentication Services or Authentication Policies, or other similar functions. A Network Administrator can view all the pages in the Status and Logs areas.
- A *Policy Administrator* can perform functions under the Rights Manager, such as adding and removing users, configuring Authentication, setting up Identity Profiles, Connection Profiles, and Access Policies, and manipulating the Rights Assignment Table. A Policy Administrator cannot modify any of the network configuration parameters, or perform system software updates, backups, or restarts. A Policy Administrator can view all the pages in the Status and Logs areas.
- A *Super Administrator* can perform all the administrative functions for all connected components of a 700wl Series system—both network and rights configuration. In addition, a Super Administrator can add, delete, enable, and disable other administrator.

There is one built-in administrator that has Super Administrator capabilities. This is the only administrator that exists on a new unit. While all other administrator settings are maintained in the 700wl Series system database, and thus are deleted if the system is reset to factory defaults, the built-in administrator simply has its name and password reset to the default.

The built-in administrator name and password can be changed on the System Components Edit page for an individual system component. For information about creating additional administrator accounts, see *Setting Up Administrators* on page 6-42.

Centralized Administration

Wireless network clients connect through an Access Controller, but authentication and rights administration for these clients is handled centrally from the Access Control Server. In addition, all configuration of the Access Control Server and all Access Controllers connected to the 700wl Series system is handled through the Administrative Console running on the Access Control Server. Once you have installed an Access Controller onto your network following the instructions in the *700wl Series Quick Start Guide*, all other administration on the Access Controller is handled through the Access Control Server.

From the centralized Administrative Console on your Access Control Server you can perform the following functions:

- Monitor in real-time the status of all the 700wl Series system components
- Monitor in real-time the status of all clients logged onto the system, and monitor the status of all their sessions
- View the 700wl Series system logs
- Update access rights for clients in real-time
- Log clients out of the system
- Configure advanced network settings for 700wl Series system components, including bridging, DHCP addressing for use with NAT, IP broadcast forwarding, setting up HTTP proxies, configuring SNMP settings, and setting the system date and time

Using the 700wl Series System

- Enable or disable Wireless Data Privacy protocols, configuring the address method and range for VPN tunneling, and configuring IPSec parameters
- Update the 700wl Series system software
- Back up a 700wl Series system component's configuration, and restore the backup if needed
- Set up Connection Profiles that identify where and when clients connect to the 700wl Series system
- Set up Authentication Policies that determine how clients authenticate themselves to the system
- Set up Access Policies to control what users can do over the network
- Set up Identity Profiles to put users in groups that share the same access policies
- Customize login pages

Logging on to the Administrative Console

To monitor or configure the 700wl Series system you use the Administrative Console. This is a web-based interface. To log in to the Administration Interface over the network, follow these steps:

Step 1. Set your browser to the IP address or hostname of your Integrated Access Manager or Access Control Server.

For example, if the IP address of your Access Control Server is 10.2.3.4, you can access its Administrative Console by entering `http://10.2.3.4` in the address or location textbox of the browser software.

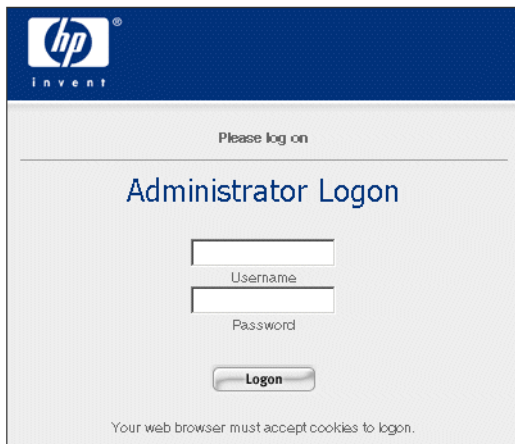
The Administrator Logon page appears, as shown in Figure 2-1.

Note: Your browser must accept cookies to enable logging on.

Step 2. Enter your administrator name and password and click **Logon**.

The initial administrator name is "admin" and the initial password is "admin."

Figure 2-1. Administrator Logon Page



The Administrative Console initially displays the Equipment Status tab under the Status module.

Note: It is strongly recommended that you change the built-in administrator logon name and password as soon as possible. You should also set the date and time for each 700wl Series system component (Access Control Server, Integrated Access Manager, and Access Controllers).

Changing the Built-In Administrator Username and Password

To change the built-in administrator name and password on a 700wl Series system unit do the following:

- Step 1.** Click the **Network** button in the Navigation bar. The System Components page appears, with a System Components list that shows the components that make up your 700wl Series system.
- Step 2.** Click a system component name listed under the Component Name heading to bring up the Edit page.
- Step 3.** In the **Admin Username** field, type a new administrator user name.
Type a new password in the **Admin Password** field, and type it again in the **Confirm Admin Password** field.
- Step 4.** Click **Save**.

You can make other changes on this Edit page, such as giving the unit a descriptive name, changing the shared secret, and so on. See *Configuring an Access Control Server* on page 6-3, *Configuring an Integrated Access Manager* on page 6-7, or *Configuring Access Controllers* on page 6-10 in Chapter 6 for more information on changing these settings.


Note: When a 700wl Series system unit is reset to its factory default settings, the built-in administrator logon name and password are also reset to their defaults.

The built-in administrator for an Access Control Server or Integrated Access Manager has the equivalent of Super Administrator capabilities—this administrator can configure all network and Rights settings for the Access Control Server or Integrated Access Manager as well as perform configuration through the Administrative Console for any Access Controllers connected to the Access Control Server or Integrated Access Manager. The built-in administrator for an Access Controller can only log on to that Access Controller through the Command Line Interface (CLI).



You can create additional 700wl Series system administrators on the Access Control Server or Integrated Access Manager, with different administration roles—Super Administrators, Network Administrators, and Policy Administrators. See *Setting Up Administrators* on page 6-42 for information about creating additional administrators.

Using Online Help


The 700wl Series system offers several levels of Help:

- Each page of the Administrative Console includes some basic Help, normally displayed in the left panel under the page name (and beneath the System Components List or page links, if they are present on the page).
- The Help button  displays context-sensitive help presented in a separate browser window. The contents of this page are different depending on the page of the Administrative Console you are viewing when you click **Help**. Once inside the help system you can move around to view different topics using a variety of navigation tools:
 - Next/previous page buttons

Using the 700wl Series System

- Links within the page contents
- Related Topics links: these are presented at the top of the page, or they can be accessed from a Related Topics menu displayed using the Related Topics button 
- Table of Contents and Index, accessed through the navigation panel at the left of the page.
- You can display the Table of Contents by clicking the Contents button 

You can also print the page you are viewing by clicking the print button .

- From the Help window, you can display the full 700wl Series system Management and Configuration Guide by clicking the PDF button ().

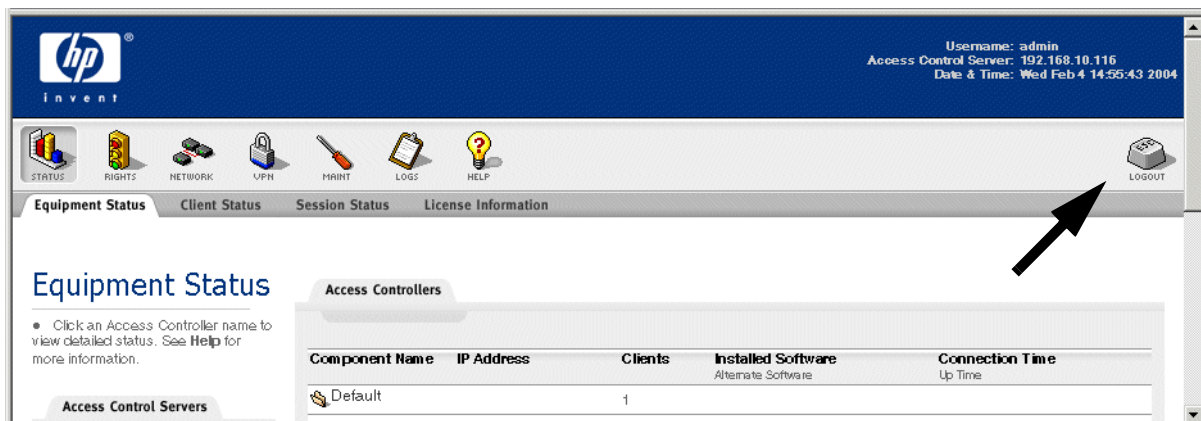
This requires a version of Adobe's Acrobat Reader software, which is available free of charge from Adobe Systems at <http://www.adobe.com>.

Logging Out

To log out of the Administrative Console:

- » From any page, click the Logout button at the right of the Navigation bar. See Figure 2-2.

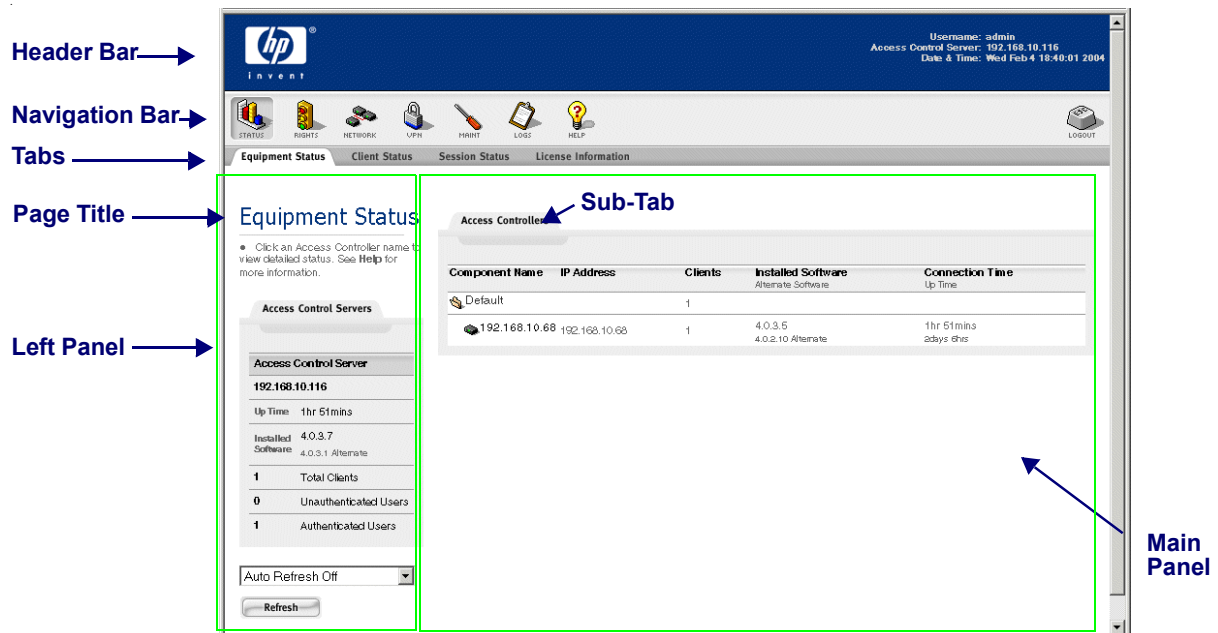
Figure 2-2. Logging Out



Using the Administrative Console

When you first logon to the Administrative Console, your browser displays the **Equipment Status** tab of the Status pages (Figure 2-3).

Figure 2-3. Initial Page of the Administrative Console



The various pages of the Administrative Console have many elements in common, as well as elements specific to certain pages.

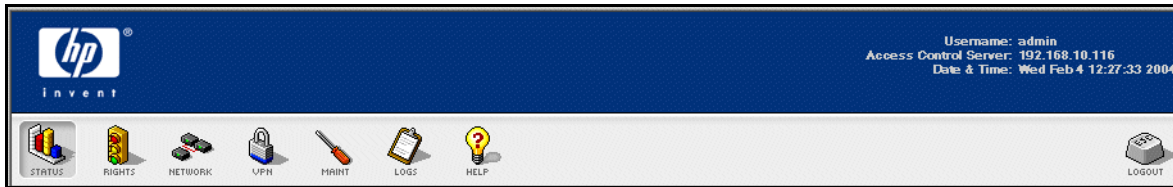
All pages have the following elements in common:

- The Header bar—Administrative Console session information
- The Navigation bar—Navigation and Logout buttons
- Tabs—Main function pages under each Navigation button containing left and main panels
- Left Panel—Instructive page information, page and component links, and data filters
- Main Panel—Input interfaces in the form of tables or sub-tabs, and tables displaying logs or status

Header Bar and Navigation Bar

The Header bar identifies the Access Control Server on which you are running the Administrative Console. The Navigation bar shows the top-level set of options provided by the Administrative Console based on the type of access the logged-in Administrator is permitted. Figure 2-4 shows the Header and Navigation bars of a single Access Control Server for an administrator with Super Admin access.

Figure 2-4. Header and Navigation Bars for an Access Control Server



Information at the right side of the Header bar shows the username of the logged in Administrator, the IP address of the Access Control Server, and the current date and time.

- If the IP address is labeled simply **Access Control Server**, this Access Control Server is functioning as the only Access Control Server in the 700wl Series system. If the system is an Integrated Access Manager, the label will reflect that.
- If the IP address is labeled **Primary Access Control Server**, this Access Control Server is currently functioning as the primary Access Control Server in a redundant configuration. You can perform all management and configuration functions for your 700wl Series system from this Access Control Server.
- If the IP address is labeled **Secondary Access Control Server**, this Access Control Server is functioning as a secondary Access Control Server in a redundant configuration. In this case, the Header bar is also labeled with a large “secondary” and only a subset of the Navigation buttons are available. (see Figure 2-5). Limited configuration capabilities are available directly through the Secondary Access Control Server.

Figure 2-5. Header and Navigation Bars for a Secondary Access Control Server



The Navigation bar is always accessible from anywhere in the Administrative Console. Each Navigation button takes you to a set of pages related to specific administrative functions.



Status

The Status pages of the Administrative Console provide views of the status of system equipment, clients, and sessions. The Equipment Status tab is displayed when a 700wl Series system administrator first enters the Administrative Console. These pages are available to administrators of all access levels.

For details, refer to Chapter 3, *System Status*.



Rights

The Rights Manager pages of the Administrative Console enable you to manage access rights for clients, customize client logon windows, and configure authentication and access control policies. These pages are available to Super Administrators and Policy Administrators. Additional tools such as simulating user rights for testing are also available.

For details, refer to Chapter 4, *Configuring Rights* and Chapter 5, *Configuring Authentication*.



Network

The Network pages enable configuration of the 700wl Series system components to work with your enterprise network. Most pages in this area are available to Super Administrators and Network Administrators only. However, both Network Administrator and Policy Administrators can change their own passwords under this function.

For details, refer to Chapter 6, *Configuring the Network*.



VPN

The VPN pages enable Wireless Data Privacy configuration, such as configuring IPSec, certificates, and IP address assignment for tunneling. These pages are available to administrators of all access levels.

For details, refer to Chapter 7, *Setting up Wireless Data Privacy*.



Maintenance

The Maintenance pages provide the following functions: Software Setup, Backup & Restore, and Shutdown/Restart of 700wl Series system equipment. These pages are available to Super Administrators and Network Administrators.

For details, refer to Chapter 8, *System Maintenance*.



Logs

The Logs pages provide views of the log data, which includes time, source, severity and event description. Log data can be filtered and exported as text files. Configure the settings for a syslog server. These pages are available to administrators of all access levels.

For details, refer to Chapter 9, *Logs*.



Help

Click this button in the Navigation bar to view context-sensitive HTML help for the tab or subordinate tab displayed. You can also access the complete *700wl Series system Management and Configuration Guide* in PDF format from the Help interface.



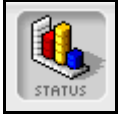





Logout

Click this button to log out of the 700wl Series system. A new logon window is displayed. You will need to log on again to perform additional system tasks with the Administrative Console.

Summary of Functions

The main administrative functions and the first level of tabs available under each Navigation button are listed below.


Using the 700wl Series System

Status	Rights	Network	VPN	Maintenance	Logs
					
<ul style="list-style-type: none">• Equipment Status• Client Status• Session Status• License Information	<ul style="list-style-type: none">• Rights Setup• Identity Profiles• Connection Profiles• Authentication Policies• Access Policies• Login Customization• Tools & Options	<ul style="list-style-type: none">• System Components• Network Setup• Interfaces• SNMP• Date & Time• Admin Setup	<ul style="list-style-type: none">• Wireless Data Privacy Setup• Certificates• IP Address Assignment (for Tunneling)	<ul style="list-style-type: none">• Software Setup• Backup & Restore• Shutdown/Restart	<ul style="list-style-type: none">• Log Files• Logging Setup

Tabs

Tabs are used to access the pages found under a Navigation button. Clicking a button on the Navigation bar displays the first (left-most) tab for that set of functions, as shown in Figure 2-3. The active tab is shown in white. Clicking an inactive tab makes it the active tab and displays the page for that subset of functions.

Some tabs represent complex sets of functions. These may use *sub-tabs* to further organize the functions and make them easier to use. Sub-tabs work the same as tabs, with the active tab shown in white and inactive tabs grayed out.

When there are action buttons, for example, the **Save** button () , displayed at the bottom of the page, the buttons pertain to the entire set of functions available under the tab. When the action buttons are displayed within the grayed area under a sub-tab, the buttons apply only to the input fields for the sub-tab.

A main tab page is divided into two distinct areas—the left panel containing informational and navigational aids, and the main panel containing the main functional area of the page (see Figure 2-3).

Function-specific elements that are common to many pages include:

- System Component list, Navigation links, or Display filters
- Input interfaces such as text fields, check boxes, buttons, drop-down lists
- Table manipulation buttons for re-ordering, editing, or deleting rows
- Page navigation controls for viewing large amounts of data spanning multiple pages
- Refresh mechanisms for updating the page, and Save, Save As Copy, Reset to Defaults, and Cancel buttons

Left Panel

The left panel contains explanatory or descriptive text about the page and its functions. It also contains controls for the features of the page, and navigation aids. The specific controls in the left panel depend on the function of the page. The left panel may contain one of the following function-specific elements:

- System Component list
- Navigation links
- Display filters

System Components List

On pages where you need to apply commands to specific HP ProCurve components (Access Control Server, Integrated Access Manager or Access Controller) a concise version of the System Components list appears in the left panel. To configure or maintain a specific component, click the component name in the System Components list to select it. The selected component appears highlighted and the page changes to display the current settings for that component. Any changes you make apply to that component.

The folders in the System Components list can be opened and closed to display the components that comprise the 700wl Series system. Figure 2-6 shows an example of a System Components list.

Figure 2-6. System Components List

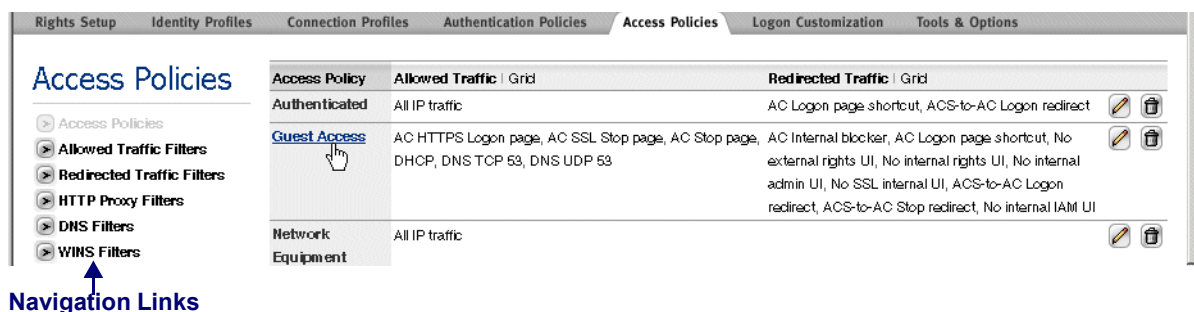


Note: In a redundant configuration, both Access Control Servers are shown in the System Components list. However, you cannot make configuration changes to the secondary Access Control Server from the Administrative Console on the primary Access Control Server, and vice versa. You must logon to the Administrative Console of the peer Access Control Server to make changes to it.

Navigation Links

On some pages you can toggle among different related functions or views of the system data by clicking one of the links available in the left panel. The active navigation link is grayed out in the list, as shown in Figure 2-7.

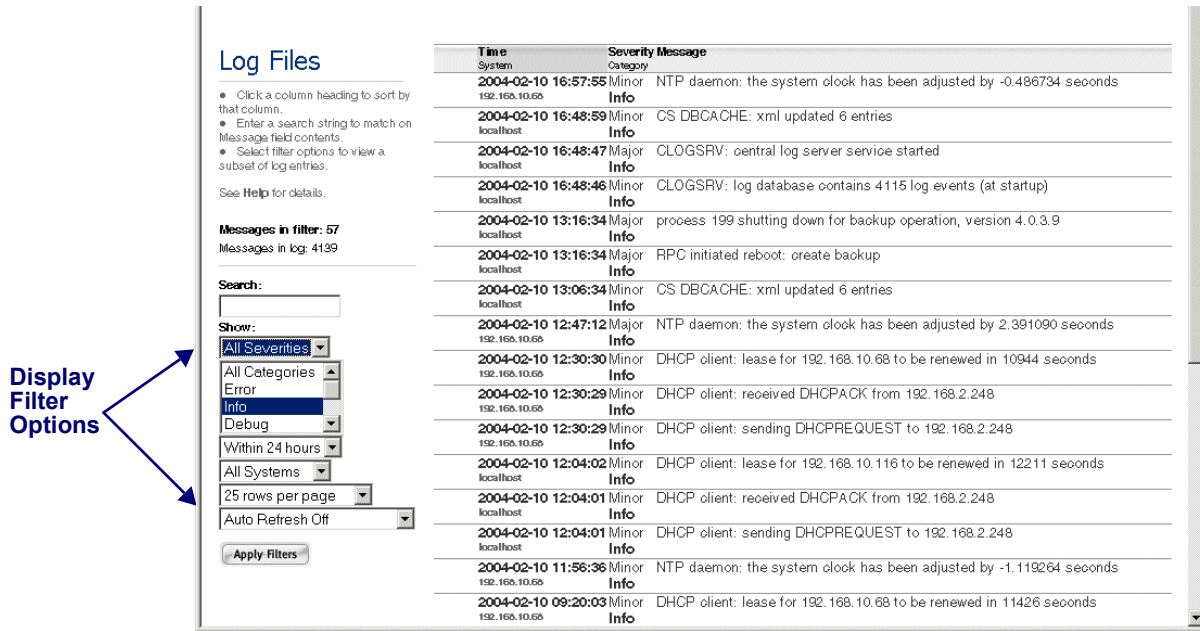
Figure 2-7. Navigation Links



Display Filters and Auto Refresh Settings

Some data, such as the contents of the log, can be very lengthy. To control the display of such information you can use filters to selectively display subsets of the total information.

Figure 2-8. Display Filters and Auto Refresh Settings



Select the desired filter values using the drop-down lists and click **Apply Filters** to refresh the display with data that matches the filter criteria. On the Log Files page, a Search capability is also provided to allow you to search for a particular string in a log file message. See Figure 2-8. On pages that display dynamic data you can set the page to automatically refresh the data at specified intervals using the **Auto Refresh** option.

Main Panel

The main panel under a tab can show two basic types of displays:

- A list or table that gives a summary view of the main elements under a tab, and may provide further navigation to view details about or manage those elements
- A set of fields, checkboxes, or buttons for configuring a particular entity of the 700wl Series system.

Tables

In configure tables, each row in a table typically displays the key items that define the element represented by the table row. For example, rows in the Rights Assignment table show the Identity Profile, Connection Profile, and Access Policy that defines the Rights Assignment row.

Configure tables, primarily those under the Rights tabs, provide the ability to edit the row definitions, add or delete rows, and edit or configure individual items within a row. Data tables, such as those under Status, provide the ability to view more detailed information about rows in the table or items within a row, but not alter the contents of the rows themselves.

Figure 2-9. Configure Tables

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the word 'invent'. The user is logged in as 'admin' with the IP address '192.168.10.116' and the date/time 'Wed Feb 4 19:34:33 2004'. The main navigation menu includes STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. The current page is 'Rights Setup' under the 'Rights Setup' tab. The table below shows the following data:

Row	Identity Profile	Connection Profile	Access Policy
1	Management	Any	Full Access
2	Engineers	Engineering	Full Access
3	Contractors	Manufacturing	MfgFloorAccess
4	Guest	Lobby	Guest Access
5	Authenticated	Any	Authenticated
6	Access Points	Any	Network Equipment
7	Any	Any	Unauthenticated

Each row in the Rights table consists of an Identity Profile (who is accessing the network), a Connection Profile (where and when the user connects to the network) and an Access Policy (what rights the user is granted). Buttons for 'New Rights Assignment...' and 'Refresh User Rights Now' are visible at the bottom of the table.

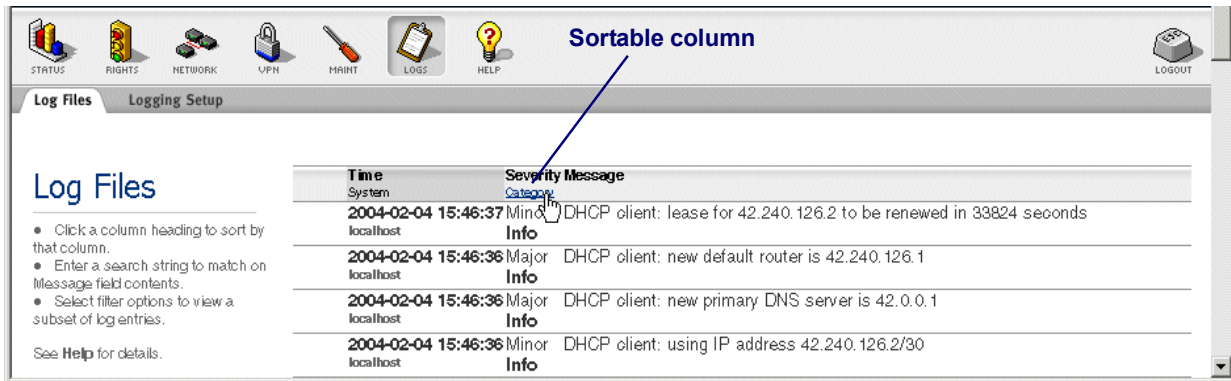
- *Manipulating rows*

To operate on rows in a table, use the buttons on the right side of the row as shown in Figure 2-9. The common buttons for editing a row (✎) and for deleting an row (🗑) are shown. See *Common Buttons* on page 2-15 for a full list of buttons.

- *Manipulating items within a row*

In some tables you can edit an item in the table by clicking on that item. Row items that can be edited or configured appear as a link when the cursor is rolled over the item. An example of this is shown in Figure 2-9 where the "Manufacturing" link under the Connection Profile column is highlighted.

Figure 2-10. Data Tables



- *Sortable Column Headings*

In some tables you can sort the items in the table based on the table columns. Column headings that allow sorting appear as a link when the cursor is rolled over the column name, as shown in Figure 2-10. In some tables, such as the Log Files display, where there are multiple headings shown in a column, you can sort on each item in the column separately. This is the case with the example in Figure 2-10).

Clicking the column heading sorts the table based on the alphabetical ordering of the items in that column. Clicking the first time sorts in ascending order; clicking a second time reverses the sort order. The column that is currently determining the display order is indicated by showing the heading cell in a darker grey. In Figure 2-10 the display is ordered based on the **Time** column.

- *Page Navigation Controls*

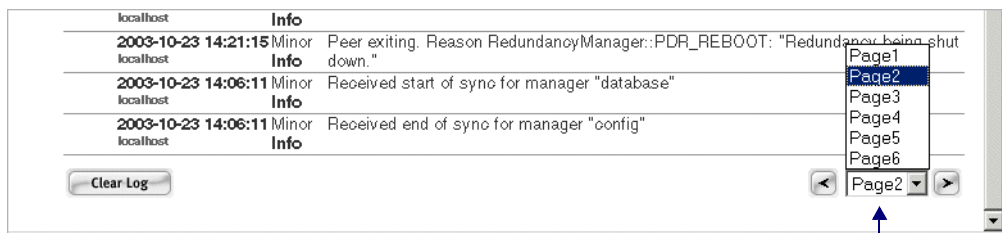
If a table contains more than 25 rows, the table is displayed in multiple pages with 25 rows per page. You can change the number of lines displayed per page using the filter settings discussed earlier. A set of page navigation controls are displayed below the bottom right corner of the table. You can navigate among the pages in two ways:

- Use the forward (▶) and backward (◀) arrow buttons to view pages sequentially.

Buttons are grayed out if you cannot move in that direction.

- Select a page number from the drop-down list (Page 1 ▾) to go directly to a specific page.

Figure 2-11. Page Navigation Controls










Page Navigation Controls

Common Buttons

The following table lists the common buttons used in the Administrative Console and gives their meaning.

Table 2-1. Administrative Console Buttons

Button	Function
	Folder: This represents a user-defined folder for system components. Folders can be opened, revealing their contents, by clicking on the open folder button (☰). They can be closed by clicking on the close folder button (☐). This button appears in the System Components List. See the example in Figure 2-6.
	Edit: Click this button to edit the object in the same row. If the item cannot be edited, the button is dimmed. See Figure 2-9 for an example of this button.
	Remove: Click this button to delete the object in the same row. If the object in the row cannot be deleted, the button is dimmed. See Figure 2-9 for an example of this button.
	ReOrder: Click the up or down arrows to move the row up or down in the table. If the row is at the top or bottom of the table, only one arrow is enabled. If a particular row cannot be moved, the button is dimmed. See Figure 2-9 for an example of this icon.
	View: Click this button to view supporting information about a particular function. This button appears in the New/Edit Filter pages for Allowed and Redirected Traffic Filters.
	Refresh Rights: Click this button to update the rights for the client in the same row. This button appears in the Client Status table.
	Logout: Click this button to logout the client in the same row. This button appears in the Client Status table.

Basic System Configuration Tasks

When you have completed the installation of your 700wl Series system following the instructions in the *700wl Series system Quick Start Guide* or the *700wl Series system Installation and Getting Started Guide* for the components in your system, there are still some basic configuration tasks you may need to perform.

- If you have not done so already, change your administrator logon username and password. See *Changing the Built-In Administrator Username and Password* on page 2-5.
- To add users to the system and specify what access rights they should have, read Chapter 4, *Configuring Rights*.
- To specify one or more external authentication services, LDAP, RADIUS, Kerberos or XML-RPC, 802.1x or NT Domain logon, for user authentication, read Chapter 5, *Configuring Authentication*.
- To specify access policies that define permitted access for users, read Chapter 4, *Configuring Rights*.
- To enable and configure the 700wl Series system to allow access using VPN protocols, read Chapter 7, *Setting up Wireless Data Privacy*.
- Once the 700wl Series system is up and running, and you want to monitor system and client status you should read Chapter 3, *System Status*.
- When you are ready to back up your 700wl Series system configuration, read *Backing Up and Restoring the System Configuration* in Chapter 8, *System Maintenance*.
- If you want to upgrade the 700wl Series system software, read *Updating the System Software* in Chapter 8, *System Maintenance*.

Setting Up Authentication and Access Rights

Chapter 4, *Configuring Rights* and Chapter 5, *Configuring Authentication* together explain the Rights Manager and should be read together since access rights and authentication are closely related.

To do the following:

Add users to the built-in database for user authentication
Add the MAC addresses of APs or other network devices
Create an Identity Profile
Configure an authentication service
Define an Authentication Policy
Define a Location
Define a Time Window
Create a Connection Profile
Define or modify an Access Policy
Add an entry to the Rights Assignment Table
Customize the Logon page
Customize the Stop page

Go to:

Creating or Editing a User on page 4-17
Creating or Editing an Equipment Entry on page 4-22
Creating or Editing an Identity Profile on page 4-13
Configuring Authentication Services on page 5-7
Creating or Editing an Authentication Policy on page 5-6
Locations on page 4-35
Time Windows on page 4-37
Creating or Editing a Connection Profile on page 4-31
Creating or Editing an Access Policy on page 4-43
The Rights Assignment Table on page 4-6
Customizing a Logon Page on page 5-32
Customizing the Stop Page on page 5-37

System Features and Concepts

The following sections provide an introduction to some of the key concepts and functions that are central to the 700wl Series system. Many of these concepts are discussed in more detail in the appropriate chapters later in this Guide. However, some of the discussions below do require an understanding of other concepts such as how Access Rights are defined and administered in the 700wl Series system.

Centralized Management and Administration

All configuration, management, and monitoring of the components of the 700wl Series system, with very few exceptions, are done through the centralized Administrative Console, accessed through the Access Control Server. The Access Control Server maintains the status and configuration information for the Access Controllers it serves. When changes are made to an Access Controller configuration, the change is saved on the Access Control Server as well as being propagated to the Access Controller.

The only configuration that should be performed directly on an Access Controller is setting the initial network configuration when the unit is first installed on your network. This is necessary to enable the Access Controller to communicate with the Access Control Server, and should be performed through the CLI.

As soon as an Access Controller is configured to communicate with its Access Control Server, that Access Controller will appear in the System Components list on the Access Control Server. By selecting the Access Controller in this list you can perform configuration and management functions such as setting the date and time, configuring options such as bridging, port subnets, SNMP access, and so on. You can also initiate upgrades, and shut down or restart the unit through the centralized interface. System-wide backups are performed from the central Administrative Console. In addition, status information such as client and session status, is gathered from the Access Controllers and is maintained and displayed centrally. Log entries are also stored centrally rather than on each Access Controller.

Because configuration information for an Access Controller is maintained by the Access Control Server, configuration changes must **not** be made directly on an Access Controller. Changes made directly on the Access Controller are not reflected in the central database, and those changes would be overwritten the next time the Access Control Server propagated configuration information to the Access Controller.

In earlier versions of the 700wl Series system, it was possible to access an Administrative Console on an Access Controller by pointing a web browser to the IP address of the Access Controller. This is no longer supported—instead the Access Controller just displays a page with a link to the Access Control Server Administrative Console, as shown in Figure 2-12.

Figure 2-12. Access Controller Redirect Page



Enterprise Class Redundancy

The 700wl Series system supports Access Control Server redundancy and failover. Access Control Server failover provides high availability operation for clients in case of system outages, network failures, or other disruptions. The primary Access Control Server functions as a normal Access Control Server, servicing the connected Access Controllers' requests for authentication, rights administration, and other functions. The redundant Access Control Server is synchronized with the primary Access Control Server through a combination of database replication, message and state replication, and configuration replication, and is kept synchronized via incremental SQL updates.

To set up a redundant Access Control Server, the following is required:

- Two peer Access Control Servers, each running version 4.0 or later software, must exist on the network and be mutually reachable. Integrated Access Managers cannot be used as redundant peers.
- One of these Access Control Servers must have the **Preferred Primary Access Control Server** option checked as part of the Access Control Server setup under the System Components tab of the Network pages. *Only one of the peer Access Control Servers may have this option checked.*
- Both Access Control Servers, and all Access Controllers, must be configured with the same shared secret in order to communicate with each other.
- As Access Controllers are installed on the network, they are configured with the IP address of the Preferred Primary Access Control Server. Access Controllers in a system with redundant Access Control Servers receive the address of the secondary Access Control Server from the Primary Access Control Server.

See [Configuring Failover with Redundant Access Control Servers](#) on page 6-15 in Chapter 6 for details on configuring redundant Access Control Servers.

How Access Control Server Failover Works

When a redundant relationship is established, the primary Access Control Server initially replicates its configuration state and database on the secondary Access Control Server. From then on, SQL updates will keep the secondary Access Control Server synchronized with the primary Access Control Server. A "heartbeat" message between the primary and secondary is used to keep the secondary Access Control Server informed that the primary is functioning.

The communication between the two peer Access Control Servers is done via a proprietary message based protocol over TCP/IP.

Upon restart, an Access Controller attempts to communicate with the primary Access Control Server. If that fails, the Access Controller attempts to communicate with the secondary Access Control Server.

In the event of a primary Access Control Server failure, or failure on the network segment on which it resides, the secondary Access Control Server will fail to receive the heartbeat message. A failover timeout is used to determine when it is appropriate for the secondary Access Control Server to take over management of the 700wl Series system. Depending on the nature of the failure, this may work in one of several ways:

- If the primary Access Control Server has actually failed or gone offline, the Access Controllers it was administering will no longer be able to contact it. They will then attempt to establish communication with the secondary Access Control Server. This Access Control Server will become the primary Access Control Server, and the failed Access Control Server, when it comes back online, will be the secondary Access Control Server.
- If the loss of heartbeat is due to a failure or disruption of the network between the two Access Control Servers rather than a failure of the primary Access Control Server itself, the Access Controllers that reside in the same partition as the primary Access Control Server will continue to communicate successfully with that Access Control Server. Access Controllers in the other network partition will establish connections with the secondary Access Control Server, which will become the primary Access Control Server to those Access Controllers.

When an Access Control Server failover occurs, authenticated clients on the various Access Controllers will continue to have access to the network and will not be aware of the failover.

Access Control Server failover to the secondary Access Control Server is automatic. Return of control to the primary Access Control Server is a manual process. This allows the system administrator time to diagnose and repair the network failure or problem with the primary Access Control Server before returning control. Once the primary Access Control Server is back on-line the two Access Control Servers automatically synchronize their data. The system administrator can manually return control to the original primary Access Control Server by restarting the new primary Access Control Server (originally the secondary) to force a fail-back to the original (Preferred Primary) Access Control Server. This is done through the **Shutdown/Restart** tab under the **Maint** navigation button.

The overall time required for a failover to occur is a function of several factors:

- The time interval specified in the **Failover Timeout** field in the Edit Control Server page
- The latency in the network link between the primary and the secondary Access Control Servers

If the primary and secondary Access Control Servers are located together with a hardwired link between them, the overall failover time can be as small as one second. If they are located thousands of miles apart then the latency time for communication between the two Access Control Servers may become significant.

Avoiding Configuration Data Loss in a Redundant System

When setting up a redundant configuration for Access Control Server failover, there are a few situations where it is possible to experience the loss of some configuration data.

The first situation is if you designate an Access Control Server as secondary when it still has valid configuration data. For example, if it is actively managing an Access Controller with connected clients,

Using the 700wl Series System

or has some other configuration information you would prefer not to lose. The act of making it a secondary Access Control Server in an active redundant peer relationship will cause its configuration to be overwritten by the Primary Access Control Server configuration. This situation can be avoided by backing up the configuration of the peer Access Control Server, and double-checking your peer configuration before enabling redundancy.

The second situation where data loss may occur is if a failover event occurs before the initial data synchronization between the redundant Access Control Servers has completed. In this case, the secondary Access Control Server will not have complete information to be able to take over as a fully functional primary Access Control Server. Because synchronization happens quickly the likelihood of data loss for this reason is small.

The third situation involves a loss of connectivity between the primary and secondary Access Control Servers. In this situation there is no power failure of the Preferred Primary, instead the Secondary does not detect a heartbeat message from the Preferred Primary due to the loss of connectivity and promotes itself to primary. Now there are two primary Access Control Servers managing the 700wl Series system. If an administrator attempts to access the Preferred Primary and cannot due the loss of connectivity affecting that connection, then the administrator will assume there was a failover and access the secondary Access Control Server now assumed to be the primary. If configuration changes are made to the previously secondary Access Control Server during the loss of connectivity they will be lost when connectivity is restored and the Preferred Primary again assumes its role and overwrites the configuration data in the secondary Access Control Server with its own.

Configuration changes should only be made to the Preferred Primary. If a failover occurs, diagnosing and repairing the reason for the failover should be performed before any configuration changes are made.

Bandwidth Management

700wl Series system version 4.0 provides bandwidth rate limiting on a per-client basis. Each client may use bandwidth as necessary up to the upstream or downstream limit set by the Access Policy currently in force for that client. This implementation does not attempt to shape bandwidth usage, just enforce a per-client cap.

Because bandwidth limits are set in the Access Policy, you can set different limits for different sets of clients even if they are connecting through the same physical port. The bandwidth limit is imposed per client—even if there is additional bandwidth available on the specific port, a given client will be limited to the specified limit, and cannot take advantage of the additional unused bandwidth.

For example, suppose you select a bandwidth limit of 1Mbps (upstream and downstream) for an Access Policy named Sales. Once this is done, each user that gets rights via the Sales Access Policy will receive a bandwidth limit of 1Mbps. The 700wl Series system algorithm does not apply an overall cap to a group of users. This means you cannot, for instance, define a 10Mbps limit for the Sales Access Policy and allow all users affected by that Access Policy to freely use bandwidth within that limit. Since a WLAN is a relatively low bandwidth shared medium and the purpose of a bandwidth cap is to prevent a single user from choking all access to other users on the same AP, it generally does not make sense to set per user limits above 1.5Mbps since most APs only support total actual bandwidth between 5 and 25Mbps.

For non-TCP traffic, bandwidth limits work in a straightforward manner. For TCP traffic there are some performance considerations that may limit the throughput to less than the configured limit, especially if client traffic is being encrypted via IPSec or PPTP.

If a client is logged onto the 700wl Series system using PPTP or IPSec encryption, overhead related to packet encryption can reduce the actual throughput experienced relative to the specified throughput. If encrypted traffic is tunneled between Access Managers due to client roaming, throughput may be further affected. When a client roams between Access Managers, existing client sessions are tunneled through the new Access Manager back to the original Access Manager. For non-encrypted traffic, new sessions initiated after the roam are handled directly by the new Access Manager, but even new sessions involving encrypted traffic are tunneled back to the original Access Manager. For non-encrypted traffic that is tunneled, bandwidth limits are enforced both on the new Access Manager (to avoid tunneling packets that should be dropped) and on the original Access Manager, which makes the actual determination of whether to drop packets. However, with encrypted packets the new Access Manager cannot determine which packets should be dropped and thus tunnels all to the original Access Manager.

If the 700wl Series system is used to pass through encrypted traffic and is not the termination of the VPN, the bandwidth limitation algorithm cannot use the packet contents to help determine which packets to drop. In this case, it adopts a very conservative algorithm to ensure that throughput will not exceed the configured limits, and may in fact result in a throughput that is below the configured limits.

In general, when setting bandwidth limits you may need to adjust your bandwidth settings based on actual client experience. If clients are experiencing bandwidth significantly below the configured limits, you may want to increase the limits so that throughput more closely approaches the limits you intend.

Note: *If you are measuring throughput at layer 2, you must take into account headers, acknowledgements and other overhead, in addition to the data itself. For example, transferring a 10 megabit file via FTP at 1 megabit per second will take more than 10 seconds due to the additional information involved in the transfer.*

Addressing 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 in the subnet configured for NAT (by default, the 42.0.0.1 subnet). Packets sent by the client have their private IP address and port replaced with the IP address of the Access Controller and a port number that is unique within the 700wl Series system (NAT and PAT functions). Packets received by an Access Controller from the network sent in reply to the NAT/PAT packets are relayed to the appropriate client with the destination IP address and port number rewritten as appropriate. The Access Controller maintains a connection table to map return packets back to their destination.
- **Real IP mode** (also known as dynamic IP mode): The client sends a DHCP request for an IP address to the Access Controller, which the Access Controller passes on to an external DHCP server. By default, (no port subnetting is configured) this DHCP request obtains an IP address on the Access Controller's subnet. Subsequent packets received by the Access Controller with that IP address as the destination 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.
- **Static IP mode:** The client uses a pre-assigned IP address, which must be on the Access Controller's subnet. Packets received by the Access Controller with this static IP address as the destination 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.

Using the 700wl Series System

You specify the addressing mode for a client through the Access Policy. The 700wl Series system default is NAT mode.

Note: *If PPTP or L2TP is enabled in the Access Policy, then the NAT setting only affects how the inner tunnel address is assigned. The outer tunnel address is always NAT'ed. See the discussion in NAT and VPN Tunneling on page 2-23 for a more detailed explanation of how this is handled.*

The NAT settings affect client IP addressing as follows:

- If NAT is required (the Access Policy NAT setting is **Always**) 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's internal DHCP server, and are then translated.
- If NAT is not required, but is allowed (the Access Policy NAT setting is **When Necessary**) then the client's real or static IP address is used unless the IP address is not valid. Client DHCP requests are satisfied by the external DHCP server, and the resulting address is used. A static IP addresses is used as is, unless it is determined to be 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 configured for it (through the Subnet tab under Interfaces in the Rights Manager) then an IP address is valid if it falls within that range. If the address does not fall within the port's address range, the address is considered invalid, and 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 Controller's subnet. NAT is used only if the address is not within that subnet.

If the IP address is not valid, the Access Controller assigns a private IP address and rewrites the source address in packets. With this setting it is possible that a NAT address might be used initially, but when the client's DHCP lease expires, it might successfully get a valid real IP address, which would be used as the source IP instead of a NAT address.

- If NAT is *never* allowed (the Access Policy NAT setting is **Never**) the Access Controller or Integrated Access Manager always uses the client's real IP address (as obtained via DHCP) or its static IP address. If the address is valid (falls within the port subnet range if one is defined, or else within the Access Controller's subnet range), the address is left untouched as the source address in packets going to the network. If the client's IP address is not valid, however, traffic to and from the client is dropped.

Caution: *This setting is intended for use only in special cases. It should not be used for normal clients, including Access Points and other devices.*

Note: *It is recommended that you configure your IP address mode consistently across Access Policies that are related. For example, you should use the same NAT mode in the Access Policy you configure for unauthenticated clients and in the Access Policies that will affect those clients after they have authenticated.*

Although NAT is used by default in the 700wl Series system, you can elect whether to use NAT or to allow real IP addresses, depending on your application. Allowing the 700wl Series system to use NAT has several benefits, especially in relation to roaming:

- NAT makes roaming much more efficient. Because each NAT address is unique across the entire 700wl Series system, when the client roams to a different Access Controller its sessions can actually be moved to the new Access Controller rather than being tunneled back through the original Access

Controller. If the client is using a real IP address, all sessions must be tunneled back through 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.

There is one case where NAT will always be used, regardless of the NAT setting specified by the Access Policy and that is when PPTP/L2TP is enabled as an encryption protocol.

NAT and VPN Tunneling

The use of VPN tunneling affects IP addressing and NAT. If PPTP or L2TP is enabled for an Access Policy, then addressing works as follows:

- The initial DHCP request is taken to be a request for an outer tunnel address, and NAT is *always* used regardless of the NAT setting in the Access Policy.

Note: *A side-effect of this behavior is that if encryption is “Allowed but not Required” in the Access Policy, and a client connects without using a tunneling protocol, that client will always receive a NAT’ed IP address upon making a DHCP request. The client will avoid being NAT’ed 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 Access Policy NAT setting, 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.

Layer 3 Roaming Support

One of the key features of the 700wl Series system is its support of layer 3 roaming—enabling clients to move physically between access points without having to reauthenticate or lose their existing sessions.

Because the 700wl Series system identifies clients by MAC address, it is simple to detect when a device roams. A *Linger Timeout* determines the length of time a client has to complete a roam, that is to appear at a new physical location after disappearing from the old physical location. The settings for timing out a roaming client are part of the client’s assigned Access Policy; different clients can have different settings and a given client can have different settings depending on their location, time of day, and so on. Configuring the Linger Timeout is discussed in Chapter 4, under Access Policies: *The Timeout Tab* on page 4-59.

If the client completes the roam before the linger time has expired, 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.

Using the 700wl Series System

How the 700wl Series system handles roamed sessions depends on the protocol used by the client 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.
- If the client is using a "real" IP address (either via DHCP or a static IP address) then *all* connections are tunneled back to the original Access Controller.
- If the client is connected using PPTP or L2TP, the PPTP/L2TP session as a whole is tunneled back to the original Access Controller.

Network Address Translation and Roaming

Based on the default Access Policy configuration, 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 addresses 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.

VLANs and the 700wl Series System

The following discussion assumes that you have read [Chapter 4, *Configuring Rights*](#) and are familiar with Connection Profiles, Access Policies, and how rights are assigned to a client in the 700wl Series system.

The HP System provides support for Virtual LAN (VLAN) tagging in several ways:

- A client can be matched to a Connection Profile based on the VLAN ID (802.1Q tag) associated with the client traffic
- The VLAN tag associated with client traffic can be preserved, stripped, or rewritten before the traffic is forwarded onto the network, based on the Access Policy in force for the client.

Matching a client to a Connection Profile based on VLAN tag effectively enables you to assign an Access Policy to clients in a specific VLAN. Clients connected to the 700wl Series system always match a Connection Profile—by default this is the "Any" Connection Profile, which is defined as all Access Controller ports, 24 hours a day, seven days a week, with any VLAN tag. Optionally you can create a Connection Profile that clients will match only if their traffic matches a specific VLAN tag or is untagged. For example, Figure 2-13 shows the configuration of a Connection Profile to match traffic tagged as VLAN 10.

Figure 2-13. Connection Profile for Traffic Tagged with VLAN 10

hp invent Username: admin
Access Control Server: 192.168.10.82
Date & Time: Tue Jan 13 17:11:56 2004

STATUS RIGHTS NETWORK UPN MAINT LOGS HELP LOGOUT

Rights Setup Identity Profiles **Connection Profiles** Authentication Policies Access Policies Logon Customization Tools & Options

New Connection Profile

Provide a name for the Connection Profile, then select the settings, locations, and time windows to be included.

- On the **Settings** tab select the Logon page and Authentication Policy to be used, specify whether to match on an 802.1q VLAN tag, and whether to limit logons.
- On the **Locations** tab select the Locations to include.
- On the **Time Windows** tab select Time Windows to include.

When finished, click Save.

Name

Settings Locations Time Windows

Select a Logon page and Authentication Policy for this profile. To match on a VLAN tag, or to limit the number of users that can log on, specify it here. See **Help** for more details.

Logon Page

Authentication Policy

VLAN Identifier

Match any VLAN tag

Match on no VLAN tag

Match on this VLAN tag:

Maximum User Logons

You can then define an Access Policy that should apply to these clients and create a new row in the Rights table that associates the Access Policy with the VLAN-specific Connection Profile. For the purpose of this example, assume that the client matches the “Authenticated” Identity Profile, meaning it has been successfully authenticated with no other Identity Profile information provided. Figure 2-14 shows how you might set up the Rights table to match clients in either VLAN 10 or VLAN 20.

Figure 2-14. Rights Table with VLAN Traffic Configured

hp invent Username: admin
Access Control Server: 192.168.10.82
Date & Time: Tue Jan 13 17:16:02 2004

STATUS RIGHTS NETWORK UPN MAINT LOGS HELP LOGOUT

Rights Setup Identity Profiles Connection Profiles Authentication Policies Access Policies Logon Customization Tools & Options

Rights Setup

Rights assignments allow you to control user access rights depending on who they are and when and where they connect to your network. A client's rights are determined by the first row it matches in the Rights Table.

Each row in the Rights table consists of an Identity Profile (*who* is accessing the network), a Connection Profile (*where* and *when* the user connects to the network) and an Access Policy (*what rights* the user is granted).

Row	Identity Profile	Connection Profile	Access Policy
1	Authenticated	VLAN20clients	VLAN20clientRights
2	Authenticated	VLAN10clients	VLAN10clientRights
3	Guest	Any	Guest Access
4	Authenticated	Any	Authenticated
5	Access Points	Any	Network Equipment
6	Any	Any	Unauthenticated

Using the 700wl Series System

In this case, Authenticated clients with VLAN 20 tag will match the first row in the table, and will receive access rights based on the Access Policy created for members of that VLAN. Authenticated clients in VLAN 10 will not match the first row, but will match the second row, and receive access rights accordingly. Authenticated clients that do not use either of these VLAN tags will fall through to the third row and get the default set of rights for Authenticated users.

The Access Policies associated with the VLAN-specific Connection Profiles can be configured to modify the VLAN tagging of these clients, if necessary. By default, the tag associated with the client's traffic is removed so the client's traffic is sent on to the network untagged. This scenario can be useful if you want to use the client's VLAN membership only to assign access rights for the client, and once the Access Policy is in place, the VLAN tag is no longer important. Optionally you can configure the Access Policy to preserve the tag or you can replace the original tag with a different tag.

Note: *In the example above, unknown (unauthenticated) clients will match the "Any" Connection Profile, and thus will receive their initial logon rights and IP address assignment **without regard to their VLAN**. Only after they have been authenticated will the VLAN be taken into account in assigning the Access Policy.*

In reality, when VLANs are used in a network configuration, each VLAN is commonly associated with a specific IP subnet. The scenario described above does not accomplish that. The next section discusses how VLANs and IP addressing interact in the 700wl Series system.

VLANs and IP Addressing

Often when VLANs are used in a network environment, each VLAN is associated with a different IP subnet. The 700wl Series system provides limited support for this.

In the 700wl Series system, IP subnet ranges may be specified on a port-by-port basis. When a client connects to an Access Controller and requests an IP address (assuming Real IP is allowed by the Access Policy) the Access Controller sends a DHCP request to an external DHCP server. If a subnet range is defined for the port in question, the DHCP request specifies an address within that range.

In order to restrict an IP range to members of a specific VLAN, you can associate a Connection Profile that filters for the desired VLAN with the port that defines the subnet range. To accomplish this, you would define a Location consisting of the single port in question, create a Connection Profile that includes only that Location, and configure the Connection Profile to filter for the desired VLAN. The limitation is that all members of the VLAN must access the 700wl Series system through the single physical port that has the appropriate subnet range defined. While VLAN tag filtering is defined by the Connection Profile, IP subnet addressing is defined at the physical port level.

For example, suppose you want to have all clients that are members of VLAN 10 get IP addresses in the subnet range 192.168.150.x, and clients that are members of VLAN 20 get IP addresses in the 192.168.156.x address range. To accomplish this, you must do the following:

- Assign the 192.168.150.x subnet range to a port (for example, port 1 of slot 1) on the Access Controller. Assign the 192.168.156.x range to a different port (for example, port 2 of slot 1).
- Create two Locations—one defined as Slot 1 Port 1 and the other defined as Slot 1 Port 2.
- Create a Connection Profile that includes only the Location you just created for Port 1, and set it to "Match on VLAN tag 10." Create a second Connection Profile using the Location for Port 2, matching on VLAN 20. In the example shown in [Figure 2-15](#), these are named "VLAN10clients" and "VLAN20clients."

- Create a variation of the default “Unauthenticated” Access Policy that includes the same access rights (which basically only allow a client to request authentication) but set the NAT option to **When Necessary** and the addressing option to **Require DHCP**. In the example, this is named “UnauthenticatedRealIP”
- Make sure that the Access Policies you define for clients matching your target VLANs have the NAT option set to **When Necessary** and the addressing option to **Require DHCP**. In the example in Figure 2-15 these are named “VLAN10clientRights” and “VLAN20clientRights.”
- Create two new rows in the Rights table directly above the default row for Unauthenticated clients to map clients that match your new Connection Profiles to your new “UnauthenticatedRealIP” Access Policy (rows 6 and 7 in Figure 2-15).

Figure 2-15. Rights Table Providing VLAN Matching for Unauthenticated Clients

The screenshot shows the HP ProCurve Rights Setup interface. At the top, there is a navigation bar with icons for STATUS, RIGHTS, NETWORK, UPN, PRINT, LOGS, HELP, and LOGOUT. Below the navigation bar, there are tabs for Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies, Logon Customization, and Tools & Options. The main content area is titled "Rights Setup" and contains a table with 8 rows. The table columns are Row, Identity Profile, Connection Profile, and Access Policy. Rows 6 and 7 are highlighted. Below the table, there are two buttons: "New Rights Assignment..." and "Refresh User Rights Now".

Row	Identity Profile	Connection Profile	Access Policy
1	Authenticated	VLAN20clients	VLAN20clientRights
2	Authenticated	VLAN10clients	VLAN10clientRights
3	Guest	Any	Guest Access
4	Authenticated	Any	Authenticated
5	Access Points	Any	Network Equipment
6	Any	VLAN20clients	UnauthenticatedRealIP
7	Any	VLAN10clients	UnauthenticatedRealIP
8	Any	Any	Unauthenticated

Now, when an unknown client connects via Slot 1 Port 1, with traffic tagged as VLAN 10, that client will match Connection Profile “VLAN10clients” and based on the “UnauthenticatedRealIP” Access Policy, will receive a real IP address in the 192.168.150.x range. Clients that connect through port 2 and whose traffic is tagged as VLAN 2 will receive real IP addresses in the 192.168.156.x address range.

Any unknown clients that connect through port 1 that are not in VLAN 10, or through port 2 that are not in VLAN 20, will only match the bottom row of the Rights table. They are associated with the original “Unauthenticated” Access Policy, and will receive a NAT IP address provided you left the “Unauthenticated” Access Policy unchanged so that it specifies NAT **Always**.

The limitation is that clients in VLAN 10 will receive an address in the desired subnet range *only* if they connect through port 1, and clients in VLAN 20 will receive the correct address *only* if they connect through port 2. In any other situation, those clients will not receive an IP address in the specified range despite the presence of the correct VLAN tag in their packets. Note that you can configure the system so that these clients do receive *access rights* based on the VLAN ID as described in the first example shown in Figure 2-14.

Using the 700wl Series System

One way to work with this limitation is to place a switch between the Access Points and the Access Controller, with a separate connection between the switch and the Access Controller for each VLAN. The switch can use the SSID to determine the port to use to send traffic to the Access Controller, ensuring that traffic for each VLAN gets sent to the correct Access Controller port and each client receives an IP address in the correct address range.

SYSTEM STATUS

This chapter explains how to view the system status tables of the 700wl Series system. You can view the status of any and all system equipment (Access Controllers and Access Control Servers), clients (users, identified either by username and password or by MAC address), and sessions. You can view all the status information from one central location. The topics covered in this chapter are:

Viewing Status Information	3-1
Viewing Equipment Status	3-3
Viewing Client Status	3-7
Viewing Session Status	3-12
Viewing License Information	3-15

Further information related to system status can be obtained by looking at the log files. See “Viewing 700wl Series System Logs” on page 9-1.

Viewing Status Information

When you first logon to the Administrative Interface, the initial display is the Equipment Status tab under the Status pages, as shown in Figure 3-1.

If you are in some other section of the Administrative Interface, you can view system and client status information by clicking the **Status** icon at the top of any page on the Administrative Console.

Figure 3-1. Getting to Status Information

The screenshot shows the HP ProCurve Secure Access 700w1 Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the text 'invent'. The user information at the top right indicates 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Wed Feb 4 18:40:01 2004'. The main navigation bar contains icons for STATUS, RIGHTS, NETWORK, UPM, PRINT, LOGS, HELP, and LOGOUT. The 'Equipment Status' tab is selected, showing a detailed view of an Access Control Server. The table below shows the status of the Access Controllers.

Component Name	IP Address	Clients	Installed Software	Connection Time
Default		1	Alternate Software	Up Time
192.168.10.68	192.168.10.68	1	4.0.3.5 4.0.2.10 Alternate	1hr 51mins 2days 6hrs

There are four tabs in the status module:

- **Equipment Status** presents an overview of the status of the Access Control Servers and Access Controllers. From this page you can view a more detailed status for each Access Controller.
- **Client Status** presents a list of clients currently connected to the 700w1 Series system through the connected Access Controllers. From this tab you can refresh the access rights for one or all clients, and logout one or all clients.
- **Session Status** presents information about the active client sessions running on the 700w1 Series system.
- **License Information** displays license, copyright, and trademark information about the third-party products that are contained within the 700w1 Series system.

The page layout is similar for all three status views. For each there is a table of equipment, clients, or sessions. Each row in the table provides the status information for that item.

In both the Equipment Status and Client Status views, you can click on a component or client name in the status table to display a page with more detailed information about the status of that component or client. The sessions status table shows all the status information for each session; there is no additional information for sessions.

For both clients and sessions, you can filter the items in the table to display a subset of the complete results so that you can focus on a specific set of clients or sessions. You can focus on specific equipment in the Equipment Status table by expanding or closing folders in the list to display only the Access Controllers of interest.

If a display has more entries than will fit on one page (based on the Rows per Page filter setting), page navigation controls are enabled to let you navigate between the results pages.

In the Client Status and Session Status views, you can sort the display by the data in any column. The headings of sortable columns are actually links, and clicking the link sorts the column. Click the heading once to sort in ascending order, then click a second time to reverse the sort order. The currently sorted column is shaded to indicate that it is the one that is determining the table order. The sort order for the Equipment Status page is based on the System Components List and cannot be changed.

By default the status data present a snapshot of results as of the time the view is displayed. The results are not automatically refreshed. Clicking the **Apply Filters** button (or the **Refresh** button on the Equipment Status page) refreshes the view. You can also enable an auto-refresh that will refresh the page every 15, 30, 45, or 60 seconds.

Viewing Equipment Status

The Equipment Status tab shows the current status for the Access Control Server in the small table at the left panel of the page, and the status of all Access Controllers in the table in the main part of the page, as shown in Figure 3-2.

Figure 3-2. The Equipment Status tab

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the word "invent". The right side of the navigation bar displays the user's login information: Username: admin, Access Control Server: 192.168.10.116, and Date & Time: Wed Feb 4 18:40:01 2004. Below the navigation bar is a row of icons for STATUS, RIGHTS, NETWORK, VPN, PRINT, LOGS, HELP, and LOGOUT. The main content area is divided into tabs: Equipment Status (selected), Client Status, Session Status, and License Information. The Equipment Status tab is active, showing a sidebar on the left and a main table on the right. The sidebar, titled "Access Control Servers", displays details for the "Access Control Server" at IP address 192.168.10.116, including its up time (1hr 51mins), installed software (4.0.3.7, 4.0.3.1 Alternate), and client counts (1 Total Clients, 0 Unauthenticated Users, 1 Authenticated Users). The main table, titled "Access Controllers", has columns for Component Name, IP Address, Clients, Installed Software, and Connection Time. The table contains two rows: "Default" with 1 client and "192.168.10.68" with 1 client. The "192.168.10.68" row shows installed software versions 4.0.3.5 and 4.0.2.10 Alternate, and a connection time of 1hr 51mins and 2days 6hrs. At the bottom of the sidebar, there is an "Auto Refresh Off" dropdown menu and a "Refresh" button.

Viewing Access Control Server Status

The Access Control Server status table, as shown in Figure 3-3, shows the following information:

Table 3-1. Access Control Server status

Row	Description
(Primary/Secondary) Access Control Server	Status of the Access Control Server whose Administrative Console you are currently logged into. If this Access Control Server has been configured as part of a redundant configuration, this label indicates whether this Access Control Server is primary or secondary.
IP Address	IP address of this Access Control Server.
Up Time	The time the current system has been operational since the last reboot.
Installed Software	Current and alternate installed software versions on this system.
Total Clients	The total number of clients currently connected to the system, including both authenticated and unauthenticated clients.
Unauthenticated Users	The number of unauthenticated users—both clients that have connected and not yet been authenticated, and clients that are not required to authenticate (MAC address users and network equipment).
Authenticated Users	The number of users that have been authenticated successfully.
Secondary/Primary Access Control Server	The peer Access Control Server if one has been configured. The label indicates whether the peer is primary or secondary. This label and the following rows do not appear if no peer Access Control Server has been configured.
IP Address	IP address of the peer Access Control Server and its status: <ul style="list-style-type: none"> • Responding—the Access Control Server is configured as a peer and is up • Not Responding—the Access Control Server is configured as a peer but cannot be reached (e.g. is down, shared secret incorrect etc.) • Not Available—the Access Control Server you have configured as a peer is already in a peering relationship with a third Access Control Server and thus is not available as a peer. The IP address also functions as a link to the Administrative Console of the peer Access Control Server.
Up Time	The time the peer system has been operational since the last reboot.
Installed Software	Current and alternate installed software versions on the peer.

Figure 3-3. Access Control Server Tab for the Primary Access Control Server in a redundant configuration

Control Servers	
Primary Control Server	
192.168.10.82	
Up Time	1day 2hrs
Installed Software	4.0.4 4.0.1 Alternate
0	Total Clients
0	Unauthenticated Users
0	Authenticated Users
Secondary Control Server	
192.168.10.116	
Responding	
Up Time	22hrs 21mins
Installed Software	4.0.4 4.0.1 Alternate

Viewing Access Controller Status

The Access Controller status table displays the following information about each Access Controller:

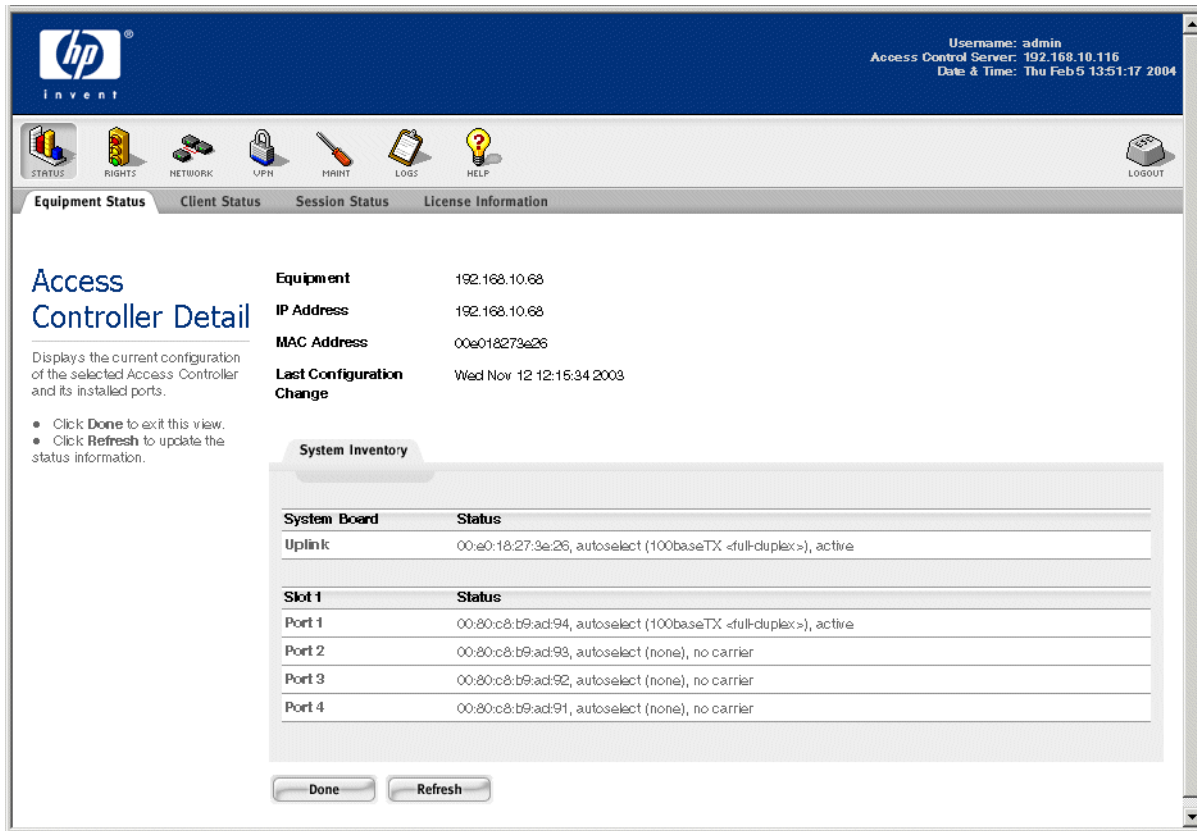
Table 3-2. Active Access Controllers Display

Column	Description
Component Name	The name assigned to the Access Controller, see “Configuring Access Controllers” on page 6-10. Click on the Component Name to view the status details for the Access Controller.
IP Address	IP Address of the Access Controller.
Clients	The number of clients currently connected to the 700wl Series system through this Access Controller.
Installed Software	The version number of the 700wl Series system software currently running on the Access Controller.
Alternate Version	The alternate version of the 700wl Series system software is shown in smaller font below this.
Connection Time	The length of time the unit has been connected to the Integrated Access Manager or Access Control Server, in days, hours, and minutes. If this Access Controller is not currently reachable, this will show “Not connected”.
Up Time	The length of time the unit has been operational since the last reboot.

Viewing Access Controller Status Details

To view the full status information for an Access Controller, click the Access Controller’s **Component Name** in the Access Controller status table. This displays the Access Controller Detail page, as shown in Figure 3-4.

Figure 3-4. Access Controller Detail Page



The Access Controller Detail page shows general status information for the Access Controller at the top of the page. Below this is a System Inventory tab that shows the status for each port on the Access Controller, grouped by slot.

Table 3-3. Access Controller Detail Page: System Inventory Display

Column	Description
Equipment	The name of the Access Controller. By default, the IP address appears as the name if the name has not been changed.
IP Address	The IP address of the Access Controller.
MAC Address	The MAC Address of the Access Controller. This is the same as the MAC address of the default Network Uplink port.
Last Configuration Change	The most recent date and time that a configuration change was made on this Access Controller.
Port Number	The port name or number, grouped by board or slot. Depending on your hardware, you may have one or two ports on the system board. Note The port currently configured as the network uplink is labeled as such. By default this is a port on the system board, but in some cases an option card port can be configured to act as the uplink port. See “Port Configuration Commands” on page A-12 for more information on configuring uplink ports.

Table 3-3. Access Controller Detail Page: System Inventory Display

Column	Description
Status	This column shows: <ul style="list-style-type: none"> The MAC address of the port The speed and duplex setting for the port, with the actual speed and duplex shown in parentheses. If the port is not connected the actual setting will be "none." The status of the connection (active or no carrier).

- » To refresh the data on the Access Controller Detail page, click **Refresh**.
- » To leave the Access Controller Detail page and return to the Equipment Status page, click **Done**.

Viewing Client Status

The Client Status page shows the status of connected clients on individual Access Controllers. Click the **Client Status** tab to view the Client Status page, as shown in Figure 3-5.

Figure 3-5. Client Status Page

The screenshot shows the HP Invent Client Status page. At the top right, it displays 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Thu Feb 5 13:52:03 2004'. The navigation bar includes tabs for 'Equipment Status', 'Client Status', 'Session Status', and 'License Information'. The 'Client Status' tab is selected. Below the navigation bar, there are icons for 'STATUS', 'RIGHTS', 'NETWORK', 'VPN', 'PRINT', 'LOGS', 'HELP', and 'LOGOUT'. The main content area features a 'Client Status' section with a table and several buttons. The table has the following data:

Client Full Name	MAC Address Machine Name	IP Address	Access Controller Slot / Port	Rights Expire
ann	00:00:86:5a:78:18	192.168.10.68	1 / 1	1wk 2days
Ann				

Below the table are buttons for 'Refresh User Rights Now' and 'Logout Users Now'. On the left side, there are instructions and filter options:

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

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



Filter options include:

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

An 'Apply Filters' button is located at the bottom left of the filter section.

Note: When the Client Status page is first displayed, it reports client information across **ALL Access Controllers**. This overview does not display the sessions or idle time for individual clients. You must select an Access Controller from the filter list and click **Apply Filters** to get this detailed information.

System Status

- » To display the client status, select the Access Controller and client type filtering parameters from the left panel and click **Apply Filters**. The display is updated to show the clients per your filter settings.
You can view full client information only on a single Access Controller at a time. The **All Access Controllers** option shows a subset of the client information.
See “Filtering Client Status Information” on page 3-9 for more information.
- » To sort the client status information click the column heading of the column you wish to sort on. For example, if you wish to sort clients by when their rights expire, click the **Rights Expire** column heading
- » To log out a specific user, click the logout icon () on the far right of the row the user is in.
To log out all users click **Logout Users Now**.
- » To refresh the rights for a specific user, click the refresh user rights icon () on the far right of the row the user is in.
- » To refresh the user rights for all clients on the Access Controller, click **Refresh User Rights Now**.
- » To look at the status details for a client, click the client name (either a logon name or an IP address) in the left column of the client status table. See “Viewing Client Details” on page 3-9 for more information.

The information in the client status table is described in Table 3-4.

Table 3-4. Active Clients Display

Column	Description
Client Full Name	The username of this client, or the MAC address if the client is identified by MAC address. This entry links to detailed information about this client. The user's descriptive name, if this client exists in the built-in User database.
MAC Address	The MAC address of the client.
Machine Name	The machine name of the client, if known.
IP Address	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.
Access Controller Slot/port	The name of the Access Controller through which this client is currently connected. The slot and port on the Access Controller through which the client is connected.
Sessions	The number of sessions currently running for this client. This is not present when the All Access Controller filter option is selected. Click on the sessions value for a client to view the Sessions Status page for that client. (This is the normal Session Status page, with filtering set to only display the session for this client.)
Idle Time	The amount of time, in minutes and seconds, that this client has been idle. This is not present when the All Access Controller filter option is selected
Rights Expire	The amount of time, in days, hours, and minutes until this client's rights expire. If the client's rights do not expire, this column will show “N/A”.

Note: If the Idle Time appears as a negative value, this means the time setting between the Access Control Server and Access Controller is not correctly synchronized.

Filtering Client Status Information

To make it easier to find the information you need from a client status page, you can filter the display to show only a subset of the entries.

- » To filter a display, select the filtering parameters from the filter drop down lists in the left panel of the status page and click **Apply Filters**. This refreshes the display with the status results based on the filtering parameters you have set.

By default Status page data is refreshed only when you click **Apply Filters**. You can set the page to automatically refresh the data at specified intervals.

- » To set the page to refresh the data at specified intervals, select the desired refresh interval from the drop down list of possible refresh rates (or select **Auto Refresh Off** to disable this) and click **Apply Filters**.

Table 3-5 shows the Client status filtering options you can use to filter the Client status display:

Table 3-5. Client Status Filtering Parameters

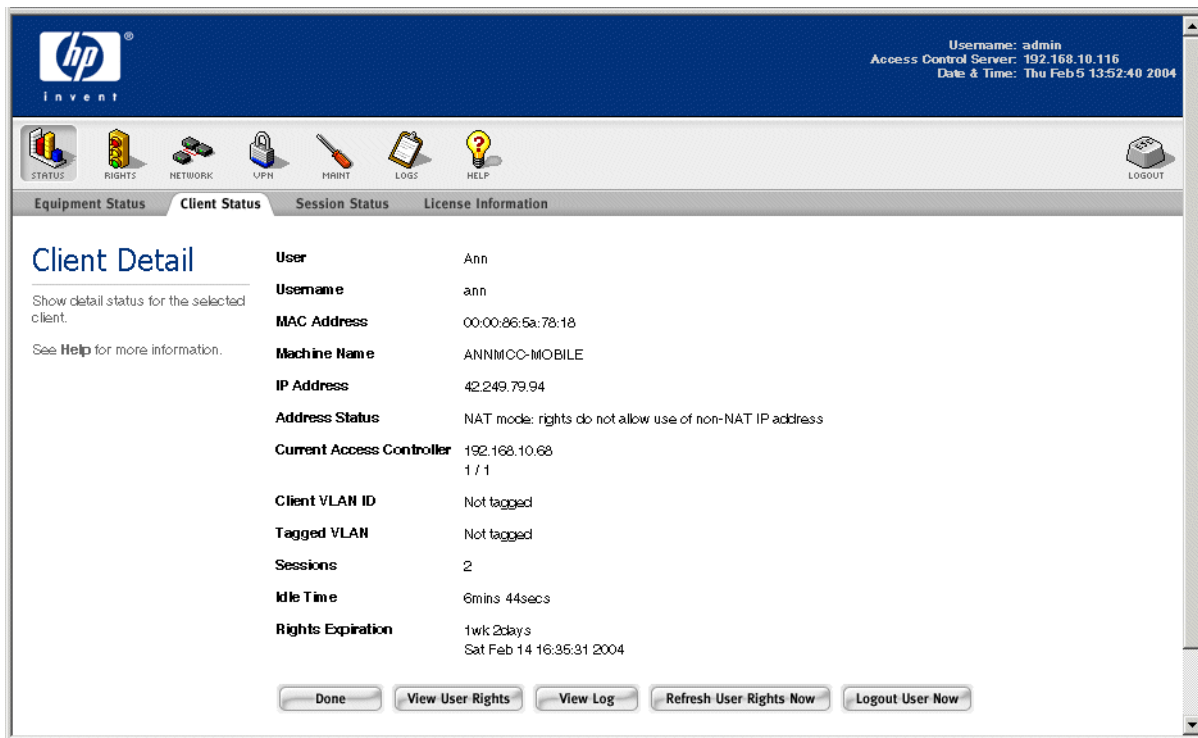
Filter by:	Details
Access Controllers	Lets you display only sessions for a selected Access Controller or for all Access Controllers. You select the Access Controller from the drop down list. Default is All Access Controllers .
Client Type	Lets you filter for: <ul style="list-style-type: none"> • All Clients. • Authenticated Clients. • Unauthenticated Clients. Default is All Clients .
Rows per Page	Lets you specify the number of rows to be displayed on a page. You can choose 25, 50, 75, or 100 rows per page. Additional results appear on successive pages. The default is 25 rows per page.
Auto Refresh	Lets you specify how often the Clients status display should be refreshed: <ul style="list-style-type: none"> • Auto Refresh Off. • Refresh every 15 seconds. • Refresh every 30 seconds. • Refresh every 45 seconds. • Refresh every 60 seconds. Default is Auto Refresh Off .

Viewing Client Details

To view details for a specific client, click the username or MAC address in the **Client** column of the Client Status table. A Client Detail page appears for the selected client, as shown Figure 3-6.

System Status

Figure 3-6. Client Detail Page



The following information is displayed on this page:

Table 3-6. Active Client detail information

Information	Description
User	The descriptive name of the user, if known.
Username	The username (logon name) of the user or the MAC address, if the user is identified by MAC address.
MAC Address	The MAC address (hardware ID) of the client.
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>"). See "IP Address Assignment for Tunneling" on page 7-11 for more information on Address Tunneling.
Address Status	Information about the IP address. This includes: <ul style="list-style-type: none">• Whether NAT mode is being used, and why.• Whether a static IP is allowed.• Other relevant information, depending on how the address was obtained.

Table 3-6. Active Client detail information

Information	Description
Current Access Controller	Information about the Access Controller through which the user is connected: <ul style="list-style-type: none"> Name of the Access Controller (by default the same as the IP address). IP address of the Access Controller. Slot and port through which the user is connected (or the port only if the unit does not provide multiple slots).
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.
Client VLAN ID	The VLAN ID on packets from the client
Tagged VLAN ID	The VLAN ID added to packets based on the Access Policy
Sessions	The number of sessions this client currently has running.
Idle Time	The amount of time, in minutes and seconds, that this client has been idle.
Rights Expiration	The amount of time, in days, hours, and minutes until this client's rights expire. If the client's rights do not expire, this column will show "N/A".

- » Click **View User Rights** to see the details of the rights for this user. The definition for this client are displayed in XML format below the rest of the status information, as shown in Figure 3-7.
- » Click **View Log** to display the log file entries for this user, filtered using the client MAC address as the search string. See "Viewing the Session Logs" on page 9-6 for more information.
- » Click **Refresh User Rights Now** to update this client's rights.
- » Click **Logout User Now** to log this client off the 700w1 Series system.
- » Click **Done** to go back to the Client Status page.

Figure 3-7. Client Detail page showing current rights in XML

Client Detail

Show detail status for the selected client.
See [Help](#) for more information.

User: Ann
Username: ann
MAC Address: 00:00:86:5a:78:18
Machine Name: ANNMCC-MOBILE
IP Address: 42.249.79.94
Address Status: NAT mode: rights do not allow use of non-NAT IP address
Current Access Controller: 192.168.10.68
 1 / 1
Client VLAN ID: Not tagged
Tagged VLAN: Not tagged
Sessions: 2
Idle Time: 7mins 23secs
Rights Expiration: 1wk 2days
 Sat Feb 14 16:35:31 2004

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

User Rights

```

<?xml version="1.0" standalone="yes"?>
<client_rights mac="00:00:86:5a:78:18" rights_id="2">
  <expiry>787333</expiry>
  <logon_time>1076005332</logon_time>
  <reauth>-12668</reauth>
  <id>ann</id>
  <vlan_id>65535</vlan_id>
  <location>
    <isNTuser>False</isNTuser>
    <locFlags>6</locFlags>
    <custName>System Customization</custName>
    <connName>Any</connName>
  </location>
</client_rights>
  
```

The Client Detail User Rights display shows the row in the Rights Table that this client matched, including the Identity Profile, Connection Profile and Access Policy associated with the client. The rest of the display shows the client's rights as defined in XML.

Viewing Session Status

Viewing session status provides information on a client's open sessions and network traffic.

- » To view active sessions, click the **Session Status** tab.

The View Active Sessions page appears, as shown in Figure 3-8.

Figure 3-8. Session Status Page

The screenshot displays the HP ProCurve Session Status page. At the top right, it shows the user is logged in as 'admin' with access control server '192.168.10.116' and the date/time 'Thu Feb 5 13:55:41 2004'. The main navigation bar includes 'Equipment Status', 'Client Status', 'Session Status' (which is active), and 'License Information'. Below the navigation, there are icons for STATUS, RIGHTS, NETWORK, UPN, PRINT, LOGS, and HELP, along with a LOGOUT button. The 'Session Status' section on the left provides instructions on how to sort and filter the data, and includes a 'Show:' dropdown menu. The main table lists active sessions with the following data:

Protocol	Idle	MAC Address	Client Source Actual Source	Client Destination Actual Destination	Slot / Port	Bytes Transmitted	Bytes Received
TCP	5 m 39 s	00:00:86:5a:78:18	42.249.79.94:1399 192.168.10.68:1399	208.45.133.133:80 208.45.133.133:80	1/1	1096	9184
TCP	5 m 34 s	00:00:86:5a:78:18	42.249.79.94:1401 192.168.10.68:1401	208.45.133.133:80 208.45.133.133:80	1/1	883	6230
TCP	6 m 25 s	00:00:86:5a:78:18	42.249.79.94:1153 192.168.10.68:1153	192.168.2.243:143 192.168.2.243:143	1/1	11498	139065
TCP	5 m 45 s	00:00:86:5a:78:18	42.249.79.94:1390 192.168.10.68:1390	192.168.10.157:139 192.168.10.157:139	1/1	626790	1095019
TCP	5 m 36 s	00:00:86:5a:78:18	42.249.79.94:1400 192.168.10.68:1400	208.45.133.133:80 208.45.133.133:80	1/1	1891	49029
UDP	5 m 45 s	00:00:86:5a:78:18	42.249.79.94:137 192.168.10.68:137	192.168.2.247:137 192.168.2.247:137	1/1	192	180
UDP	5 m 39 s	00:00:86:5a:78:18	42.249.79.94:1398 192.168.10.68:1398	192.168.2.248:53 192.168.2.248:53	1/1	62	206
UDP	5 m 34 s	00:00:86:5a:78:18	42.249.79.94:1402	192.168.2.248:53	1/1	55	

- » To filter the session data, select the desired filters and click **Apply Filters**.
- » To set an auto refresh interval, select the desired interval from the drop down list and click **Apply Filters**.
- » To set the number of rows to display per page, select the desired number from the drop down list and click **Apply Filters**.
- » To go to different pages of the session status table, use the page navigation controls at the bottom of the page on the left.

The following information is displayed on the Session Status page:

Table 3-7. View Active Sessions Information

Column	Description
Protocol	The protocol used by the session. The following protocols are translated from their numeric strings: CMP, ICMP, TCP, UDP, ESP, AH, IP, and PPTP. All other protocols are displayed as the protocol number prefixed with a pound sign (#).
Idle	The time since the last packet was received, in hours (h) and minutes (m) and seconds (s).
MAC address	The MAC address of the client associated with this session.

Table 3-7. View Active Sessions Information

Column	Description
Client Source	Client Source: The IP address and port of the client system, as placed in the packet header by the client.
Actual Source	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	Client Destination: The destination IP address as placed in the packet by the client.
Actual Destination	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	The Access Controller slot and port number used by the session (if any). For an Access Controller 720wl unit, this is just the port.
Bytes Transmitted	The total number of bytes transmitted.
Bytes Received	The total number of bytes received.

Filtering Session Status Information

To make it easier to find the information you need from a Session Status page, you can filter the display to show only a subset of the entries.

- » To filter a display, select the filtering parameters from the filter drop down lists in the left panel of the status page and click **Apply Filters**. This refreshes the display with the status results based on the filtering parameters you have set.

By default Status page data is refreshed only when you click **Apply Filters**. You can set the page to automatically refresh the data at specified intervals.

- » To set the page to refresh the data at specified intervals, select the desired refresh interval from the drop down list of possible refresh rates (or select **Auto Refresh off** to disable this feature) and click **Apply Filters**.

Table 3-8 shows the Session status filtering options you can use to filter the Session status display:

Table 3-8. Session Status Filtering Parameters

Filter by:	Details
MAC Address	Lets you display sessions for a selected MAC address or for all MAC addresses. Select a MAC address from the drop-down list. Default is All MAC Addresses .
Protocol	Lets you display only sessions using a selected protocol. You select the protocol from the drop-down list. Default is All Protocols .

Table 3-8. Session Status Filtering Parameters

Filter by:	Details
Access Controllers	Lets you display only sessions for a selected Access Controller. You select the Access Controller from the drop-down list. Default is the first Access Controller in the list.
Port	Lets you display only sessions for a selected port or for all ports of the selected Access Controller. You select the port from the drop-down list. Default is All Ports .
Rows per Page	Lets you specify the number of rows to be displayed on a page. You can choose 25, 50, 75, or 100 rows per page. Additional results appear on successive pages. The default is 25 rows per page .
Auto Refresh	Lets you specify how often the Clients status display should be refreshed: <ul style="list-style-type: none"> • Auto Refresh Off. • Refresh every 15 seconds. • Refresh every 30 seconds. • Refresh every 45 seconds. • Refresh every 60 seconds. Default is Auto Refresh Off

Viewing License Information

The License Information page shows the license, copyright, and trademark information for all third-party software used by the 700wl Series system.

- » To view version and license information, click the **License** Information tab on the **Status** pages.

Figure 3-9 shows the License Information page.

Figure 3-9. License Information Page

The screenshot displays the 'License Information' page within the HP ProCurve management interface. At the top, the HP logo and 'invent' branding are visible. The user interface includes a navigation bar with tabs for 'Equipment Status', 'Client Status', 'Session Status', and 'License Information'. The 'License Information' tab is active, showing a list of 'Third Party License Agreements'. Each agreement includes a logo, the name of the provider, and a brief description of the software included. The agreements listed are for Vernier Networks, FreeBSD, Apache, OpenSSL, and Whistle Communications. The page also contains copyright information for Hewlett-Packard Development Company, L.P. and a link to the HP ProCurve Networking web site.

hp
invent


Username: admin
Access Control Server: 192.168.10.116
Date & Time: Thu Feb 5 13:56:10 2004


STATUS RIGHTS NETWORK UPN PRINT LOGS HELP LOGOUT

Equipment Status Client Status Session Status License Information

License Information


Third Party License Agreements


 This product includes software developed by Vernier Networks Inc.
Copyright © 2001-2004 Vernier Networks Inc. All rights reserved.





Copyright © 2003-2004 Hewlett-Packard Development Company, L.P. All rights reserved.

Visit 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.

 Contains system software provided by The Regents of the University of California.
All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases are provided by The Regents of the University of California and its contributors.
Copyright 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994 The Regents of the University of California. All rights reserved.
Copyright © 1995, 1996 FreeBSD Inc. All rights reserved.

 This product includes software developed by the Apache Group for use in the Apache HTTP Server Project.

 This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.
<http://www.openssl.org/>
This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

 Some software originally written by Whistle Communications, Inc.
Copyright © 1995-1999 Whistle Communications, Inc. All rights reserved.
This software is being provided by Whistle Communications AS IS, and to the maximum extent permitted by law, Whistle Communications makes no representations or warranties, express or implied, regarding

CONFIGURING RIGHTS

This chapter describes how network access rights are assigned to clients through the 700wl Series system, and explains how to configure access control policies. The topics covered in this chapter include:

Access Rights in the 700wl Series System	4-1
The Rights Manager	4-4
Configuring Access Rights—An Overview	4-5
The Rights Assignment Table	4-6
Identity Profiles	4-11
Users in the Built-In Database	4-16
Network Equipment in the Built-in Database	4-20
Retrieving MAC Addresses from an LDAP Database	4-24
Connection Profiles	4-29
Locations	4-35
Time Windows	4-37
Access Policies	4-39
Allowed Traffic Filters	4-62
Redirected Traffic Filters	4-66
HTTP Proxy Filters	4-75
Example—Modifying the “Guest Access” Access Policy	4-79

You can configure both Authentication Policies and Access Policies through the Rights Manager. This chapter focuses on Access Policies as implemented through the Rights Assignment Table. Authentication Policy configuration is discussed in Chapter 5, “[Configuring Authentication](#)”.

Note: You must have Policy Administrator or Super Administrator access to perform the functions described in this chapter.

Access Rights in the 700wl Series System

The 700wl Series system allows network administrators to define highly flexible access control policies that grant network access to a client based on who the client is, where they connect to the 700wl Series system, and the time of day when they make the connection.

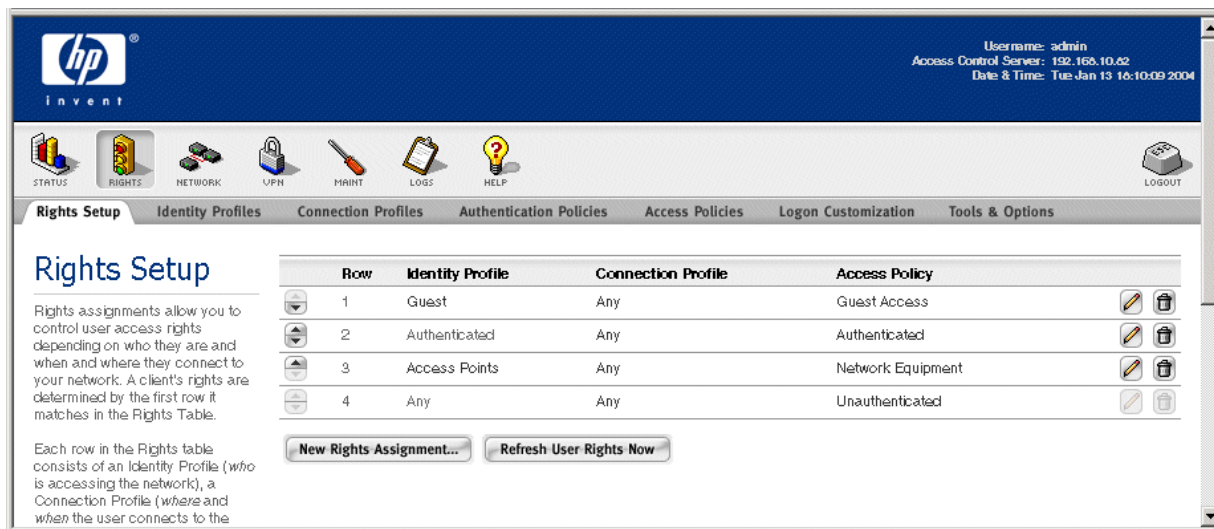
The 700wl Series system uses a client’s identity (user name or MAC address) to match the client to an *Identity Profile*. It uses the client’s Location (Access Controller port through which it is connected), the

Configuring Rights

Time Window in which the connection exists, and optionally, a VLAN tag, to match the client to a *Connection Profile*. The combination of the Identity Profile and Connection Profile determines the *Access Policy* that is used to enforce access rights (the ability to pass traffic into the network) for the client.

Access rights are implemented in the 700wl Series system through the Rights Assignment Table. Each row in the table consists of an Identity Profile, a Connection Profile, and an Access Policy (see Figure 4-1).

Figure 4-1. Rights Assignment Table—Initial Configuration



The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the word 'invent'. The user information at the top right shows 'Username: admin', 'Access Control Server: 192.168.10.42', and 'Date & Time: Tue Jan 13 16:10:09 2004'. The main navigation menu includes STATUS, RIGHTS, NETWORK, VPN, MPRINT, LOGS, HELP, and LOGOUT. The 'Rights Setup' page is displayed, featuring a table with the following data:

Row	Identity Profile	Connection Profile	Access Policy
1	Guest	Any	Guest Access
2	Authenticated	Any	Authenticated
3	Access Points	Any	Network Equipment
4	Any	Any	Unauthenticated

Below the table are two buttons: 'New Rights Assignment...' and 'Refresh User Rights Now'. The interface also includes a 'Rights Setup' section with explanatory text and a 'Logout' button.

When a client connects to the 700wl Series system, the system searches the Rights Assignment Table from the top down until it matches the client to both an Identity Profile and a Connection Profile. The Access Policy associated with the matching row determines the access rights that are granted to that client.

A client may be associated with several different Identity Profiles (and possibly different Connection Profiles) during the life of its connection to the 700wl Series system. Each time the client's identity or location changes, the 700wl Series system does a new search of the table to match the client to an Identity Profile and Connection Profile, and to determine the Access Policy it should apply as a result.

For example, when a client first connects to the system, it typically does not match any of the established Identity Profiles. The table match falls through to one of the bottom rows in the table where the new client matches on the "Any" Identity Profile. The Any Identity Profile is typically associated with the "Unauthenticated" Access Policy, which grants rights that allow the client to log on and attempt authentication. (See "Authentication in the 700wl Series System" on page 5-1 for a discussion of how authentication is handled.)

With a successful logon and authentication, the client has a new identity (its user name, and in some cases a group or domain affiliation) and now matches a different Identity Profile (for example, the "Authenticated" profile in the default case). It is granted a new set of rights based on the Access Policy in the row that matches the client's new Identity Profile and Connection Profile.

If the client roams such that its wireless connection moves to a port that is included in a different Connection Profile, a new table search occurs, and the client will match a different row in the Rights Assignment Table, based on the combination of the same Identity Profile but a different Connection Profile. This may result in a different set of rights if the Access Policy in the new matching row is different from the Access Policy in the old row.

The network administrator configures network access control policies by defining Identity Profiles, Connection Profiles and Access Policies, or by modifying existing profiles and policies.

- An **Identity Profile** is associated with a set of one or more individual users and devices, and a user may belong to more than one Identity Profile. For clients authenticated through an external authentication service, the client may match an Identity Profile if the Identity Profile name matches a group or domain name returned by the authentication process. For clients included in the built-in database, the Rights Administrator can assign those clients to Identity Profiles. The client matches the assigned Identity Profile upon successful authentication.

There are four predefined Identity Profiles: “Authenticated,” “Guest,” “Any,” and “Access Points.”

- A client that is successfully authenticated, but does not match any other Identity Profile, matches the “Authenticated” profile.
- A user that logs in as a Guest (through the web-based logon page) matches the “Guest” profile.
- A client that does not match any other Identity Profile automatically matches “Any.” The “Any” Identity Profile always appears in the last row of the Rights Assignment Table.
- The MAC addresses of Access Points and other network equipment can be added to the built-in database and associated with the “Access Points” Identity Profile. Those MAC addresses then immediately match the Access Points Identity Profile when they connect to the 700wl Series system.
- The MAC addresses of regular clients can also be stored in the built-in database as “MAC Address Users.” When these clients connect, they are recognized by their MAC address and bypass the authentication process. A MAC address user does NOT match the Authenticated Identity Profile, as they are not authenticated. If a MAC Address client has not been specifically associated with an Identity Profile in the built-in database, they will continue to match the Any Identity Profile by default.

The administrator can create additional Identity Profiles as needed. The Authenticated and Any profiles cannot be modified or deleted.

- A **Connection Profile** describes a set of physical or logical connection paths to the 700wl Series system during a specific time frame. A Connection Profile consists of one or more ports on one or more Access Controllers, Time Windows, and optionally a VLAN ID. If a VLAN ID is defined, only traffic that includes the specified VLAN tag will match the Connection Profile. The administrator can create Connection Profiles as needed to differentiate between physical locations, VLANs, and/or Time Windows. There is one predefined Connection Profile, “Any,” which includes all Access Controllers and ports, matches any VLAN tag, and is valid at all times (24 hours a day, 7 days a week). The Rights Administrator can create Connection Profiles as needed to differentiate between physical locations, Time Windows, or VLANs.

A client matches a Connection Profile if the Access Controller port through which she is connected is included in that Connection Profile, the VLAN tag associated with her packets match the VLAN ID specified for the profile, and the time at which she connects is within the Time Window defined for the profile. A client that does not match any other Connection Profile automatically matches “Any.” The “Any” Connection Profile always appears in the last row of the Rights Assignment Table.

Connection Profiles are used in two ways in the 700wl Series system:

- The Connection Profile is also used to determine the method by which an unknown (unauthenticated) client should be authenticated. This is discussed later in “Authentication in the 700wl Series System” on page 5-1.
- As discussed previously they are used in conjunction with the Identity Profile to determine the access rights granted to an authenticated client.

Configuring Rights

- An *Access Policy* defines aspects of how a client interacts with the network. The Access Policy defines what traffic is allowed to be passed into the network, and what traffic will be redirected to alternate destinations. It can include HTTP proxy filters that specify what web sites are accessible or restricted. It also defines how IP addressing is handled, and what type of encryption should be used, if any.

There are five predefined Access Policies: “Authenticated,” “Unauthenticated,” “Guest Access,” “No Access,” and “Network Equipment.” By default, the “Unauthenticated” policy appears in the last row of the Rights Assignment Table, as the policy associated with clients that fall through and match only the “Any” Identity and Connection Profiles.

The Rights Manager

The configuration of network Authentication and Access Policies is done through the Rights Manager, accessed by clicking the **Rights** icon on the Navigation Toolbar.

Configuration within the Rights Manager may include any of the following:

- Creating new rows for the Rights Assignment Table
- Creating new Identity Profiles, or modifying ones you have already created
- Creating new Connection Profiles, or modifying ones you have already created
- Creating new Access Policies, or modifying existing policies
- Creating new Authentication Policies, or modifying existing policies (this is discussed in Chapter 5, “[Configuring Authentication](#)”)
- Customizing the Logon page (and other associated pages) presented to users whose first network access attempt is an HTTP request. (This is also discussed in Chapter 5, “[Configuring Authentication](#)”)

As a part of defining the various profiles and policies, you can also define the following:

- Users (defined by a username and password or MAC address) and Network Equipment (defined by a MAC address) to be included in the built-in database. These may then be associated with an Identity Profile.
- Locations (defined as one or all ports on one or more Access Controllers). These may be used when defining Connection Profiles. By default, the location *Everywhere* encompasses all ports on all connected Access Controllers.
- Time Windows (defined as a range of hours, dates, or days of the week). These may be used when defining Connection Profiles. The absence of a specific Time Window in a Connection Profile is taken to mean no time restrictions are in force.
- Allowed Traffic Filters and Redirected Traffic Filters. These may be used when defining Access Policies. These also include the special case of WINS and DNS filters, which are created through a separate interface and result in matched Allowed and Redirected traffic filter pairs.
- HTTP Proxy Filters. These also may be used when defining Access Policies.

From the Rights Manager you can also export the current set of rights to your local system, and import a set of stored rights from the local system.

Note: *When you make a change to the rights configuration through the Rights Manager, clients are affected only when they receive new rights—rights configuration changes do **not** automatically affect connected clients. To have your changes take effect immediately for connected clients, you must go to*

the *Client Status* tab under the *Status* button, and click **Refresh User Rights Now**. You can also refresh rights for individual clients, if appropriate.

Configuring Access Rights—An Overview

To configure rights in the 700wl Series system, you first need to decide how you want to control access to the resources on your network.

Step 1. *Create Identity Profiles* to define who should have access to network resources. You can use Identity Profiles to group sets of users that should have a common set of access rights. You can also use Identity Profiles to assign access rights to network devices such as Access Points.

For example, do you want your engineers to have a different set of access rights from your accounting staff? Should instructors have different access rights than students? Do you have visitors for whom you might want to provide limited access? You can create Identity Profiles for each type of user that should have specific types of access, and then define which users belong to each Identity Profile.

You can add users to the 700wl Series system built-in database and then assign those users to Identity Profiles through the Rights Manager, or you can define Identity Profiles that will match users based on group or domain information retrieved when the user is authenticated.

- a. *Add users* to the built-in database if you don't plan to have them authenticated by an external authentication service. You can then assign them to Identity Profiles as appropriate.
- b. *Add network equipment* (such as Access Points) to the built-in database so they can be assigned a set of access rights — for example, to allow the device to be managed over the network.

Step 2. *Create Connection Profiles* to differentiate between physical locations where clients can access the system, or to differentiate between clients on different VLANs, or both. You can also use Connection Profiles to differentiate between access during different time periods.

- a. *Create Locations* that include the Access Controllers and/or Access Controller ports that provide connectivity for any specific physical locations that you want to differentiate in terms of authentication or access rights.

For example, do you want users to get different access rights when they are in building A than they get when they are in building B? Do you want students to get different access while they are in the library from those they get in a science lab? Do you want clients connecting from your corporate visitors center to be authenticated differently from clients connecting from your manufacturing floor? You can use Locations to define Connection Profiles that are unique to a specific physical location—a building, a department, a floor, a conference room.

Note: *Due to Access Point coverage overlap, Locations may not behave quite as expected if your Access Points are in close proximity. For example, if you have one Access Point connected to a port defined as Location Marketing, and a nearby Access Point defined as Location Engineering, a single, stationary user may be connected through the Marketing Location in one instance, and through the Engineering Location the next time. Such a user could even “roam” between the two Locations seemingly at random without ever physically moving.*

Note: *If your Access Controllers have not yet been installed on your network, you will not be able to use them to create Locations. However, you can still create the Connection Profiles you need with the Everywhere default location, and add Locations to the*

Connection Profiles once the Access Controllers have been installed and the appropriate Locations have been created.

- b. *Create Time Windows* that specify hours of the day, days of the week, and so on, to allow or restrict access during specified times.

For example, if you have temporary workers, or you allow guests, do you want to limit their access to normal working hours during the work week? Do you want to limit access during a particular period, such as during examinations? You can use Time Windows to define Connection Profiles that allow access only during the specified times.

You create your Connection Profiles by selecting from among the Locations and Time Windows that have been defined, or accepting the defaults. In addition, you can specify a VLAN tag to be used in matching clients to the Connection Profile. This allows you to distinguish between different groups of clients for the purposes of authentication or access rights, even though they connect through the same physical locations. You can specify that a client matches the Connection Profile only if it uses a specific VLAN tag, or if it does not use a VLAN tag (i.e. is excluded if it does use a VLAN tag). The default is that it matches with any VLAN tag.

As part of defining a Connection Profile you also specify how clients that match that Connection Profile should be authenticated. You can select an Authentication Policy individually for each Connection Profile. In addition, you can specify the logon page that should be used (either the standard logon page or a custom one) for clients that are presented with a logon page through their browser. See Chapter 5, “[Configuring Authentication](#)” for details about configuring Authentication Policies and customized Logon pages.

- Step 3.** *Create Access Policies* that define the sets of access rights you want to grant based on a client’s Identity and Connection Profile.

You can create as many Access Policies as you want. Each row in the Rights Assignment Table can have a different Access Policy, meaning you can create a different policy for every combination of Identity and Connection Profiles, if you want.

Each Access Policy is a collection of settings that include traffic filters for controlling which packets are allowed into the network, HTTP filters that determine web sites are accessible or restricted, as well as settings that specify whether encryption is required and of what type, and how IP addressing should be handled.

- *Create Allowed Traffic Filters and Redirected Traffic Filters* as appropriate to allow or restrict access to resources and destinations in your network. A number of filters for common traffic patterns are predefined, but you may find it necessary to create additional filters to meet your unique needs.

Create your Access Policies by selecting from among the traffic filters that have been defined, and by specifying other settings, such as encryption options, rights timeout values, HTTP proxy filtering, and others.

- Step 4.** *Add rows to the Rights Assignment Table* by combining the Identity Profiles, Connection Profiles, and Access Policies you’ve created. The order of these rows in the table is important, as whenever the 700wl Series system looks for a match it searches the table row by row starting from the top, and stops when it find the first match.

The Rights Assignment Table

The Rights Assignment Table is where Identity Profiles, Connection Profiles, and Access Policies come together to define the access rights granted to individual clients. Every client that connects to the 700wl

Series system is matched to a row in the table based on its Identity Profile and Connection Profile, and receives access rights as specified by the Access Policy for that row.

The 700w1 Series system looks for a matching row starting at the top of the table, and stops at the first match. Thus, the order of rows in the table is important.

In a newly-installed system (or after a Factory Reset) the Rights Assignment Table will have only four rows, as shown in Figure 4-1.

Figure 4-2. Rights Assignment Table Matching Example

The screenshot shows the HP ProCurve Rights Setup interface. At the top, there is a navigation bar with icons for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. Below the navigation bar, there are tabs for Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies, Logon Customization, and Tools & Options. The main content area is titled "Rights Setup" and contains a table with the following data:

Row	Identity Profile	Connection Profile	Access Policy
1	Accounting	Accounting	Accounting
2	Guest	Any	Guest Access
3	Authenticated	Any	Authenticated
4	Access Points	Any	Network Equipment
5	Any	Accounting	Unauthenticated
6	Any	Any	Unauthenticated

Below the table, there are two buttons: "New Rights Assignment..." and "Refresh User Rights Now".

The following examples are based on the Rights Assignment Table shown in Figure 4-2. The first example describes how a normal user (identified by a username and password) gets access rights to the system.

- Step 1.** A client connects to the 700w1 Series system and initially is identified only by its MAC address. This initiates a search of the Rights Assignment Table to match this client to a row in the table, and to assign access rights to the client based on the Access Policy specified by the matching row.
- Step 2.** Assuming this MAC address is unknown to the 700w1 Series system, the client does not match the Identity Profiles in the first four rows. It falls through to the bottom rows of the table, where it automatically matches the "Any" Identity Profile. If the client accessed the 700w1 Series system through a physical location that matches the Connection Profile "Accounting," it will match on row 5. If the client connected through any other Location, it matches on row 6. In either case the unknown client receives rights based on the "Unauthenticated" Access Policy. This Access Policy provides only the access necessary to log on to the system.
- Step 3.** Given the rights defined by the "Unauthenticated" Access Policy, when the client attempts to access any web page, she is instead redirected to the 700w1 Series system Logon page. The user can enter a username and password, or select the "Logon as a Guest" option. The logon name and password will be passed on for authentication based on the Authentication profile associated with the Connection Profile. This means that an unknown client that matches on row 5 might be authenticated differently from a client that matches row 6. (Authentication is discussed in more detail in "Authentication in the 700w1 Series System" on page 5-1.)

If the user enters a logon name and password that is authenticated successfully by the Authentication Policy, the 700w1 Series system searches the Rights Assignment Table again using

Configuring Rights

the new identification information. The user will now match one of the Identity Profiles near the top of the table. For example:

- Suppose the client initially matches row 5, (Identity Profile “Any” and Connection Profile “Accounting”) and his logon information is sent to an external authentication service such as an LDAP server. That service returns the group affiliation “Accounting” as part of the successful authentication. As a result the client matches the Identity Profile “Accounting” as well as Connection Profile “Accounting,” and gets rights based on the “Accounting” Access Policy as specified in row 1.
- Suppose a client initially matches row 5 and gets successfully authenticated, but the group information returned is *not* “Accounting.” In this case, the client does not match row 1 because it does not match Identity Profile “Accounting.” However, because it has been authenticated, it matches Identity Profile “Authenticated,” and by default matches Connection Profile “Any.” Therefore it gets rights based on row 3.
- A client that initially matches on row 6, and is successfully authenticated, also gets new rights based on row 3. Since its Connection Profile is not “Accounting”, it does not match row 1 (most likely it also does not match the Identity Profile “Accounting”).
- If the user elects to logon as a Guest, she is automatically associated with the “Guest” Identity Profile, matches on row 2 of the table, and receives rights based on the “Guest” Access Policy. Guest users are not considered authenticated by the system, and therefore do not match the “Authenticated” Identity Profile.

Note: *In this example it is important that the row containing the “Accounting” Identity Profile and the “Accounting” Connection Profile be placed **before** the row containing the “Authenticated” Identity Profile and “Any” Connection Profile. If these two rows were reversed, **all** authenticated clients would match the “Authenticated” Identity Profile and “Any” Connection Profile in the first row—including those who might also match the “Accounting” Identity Profile and the “Accounting” Connection Profile in the second row. Because the table search stops at the first match, no authenticated clients would ever get as far as the second row to receive access rights from the “Accounting” Access Policy.*

The second example describes how access rights are assigned to clients that are identified only by MAC address, where presenting a user name and password is not appropriate. Network devices such as Access Points fall into this category.

Step 1. A client connects to the 700wl Series system, identified by its MAC address. As in the first example, this initiates a search of the Rights Assignment Table. However, in this case assume that this “client” is actually an Access Point, and that the MAC addresses of all Access Points connected to the various Access Controllers have been added to the built-in database and assigned to the “Access Points” Identity Profile.




Step 2. In this case the MAC address *is* known to the system. As in the first example, the client does not match the Identity Profiles in the first three rows, but it does match the Access Points Identity Profile in row 4. This results in the client getting access rights based on the Network Equipment Access Policy. These rights do not send the client through an authentication process, and the client now has the rights it needs.

Like Guests, clients identified only by MAC address are *not* considered authenticated, and therefore do not match the “Authenticated” Identity Profile. If a MAC address user has been added to the built-in database, but has not been assigned to an Identity Profile, that client will continue to match the “Any” Identity Profile.

Note: It is important that rows with the “Access Points” Identity Profile appear in the table **before** rows that contain the “Any” Identity Profile. Otherwise, the MAC address would match “Any” first, and would never get to the row with the “Access Points” Identity Profile.

Modifying the Rights Assignment Table

You can add new rows to the Rights Assignment Table, delete rows from it, or modify the rows in the table. You can also reorder the rows in the table to create the right precedence relationships when searching for a match.

- » To add a row, click the **New Rights Assignment...** button at the bottom of the page. This displays the New Rights Assignment page, where you can select from among the existing Identity, Connection and Access Policies to define a new row for the table. See “Adding or Editing a Rights Assignment” on page 4-9.
- » To edit a row, click the Pencil icon  at the far right of the row. This displays the Edit Rights Assignment page, where you can change any of the profiles used in the row by selecting from the existing Identity, Connection and Access Policies. This page is almost identical to the New Rights Assignment page, except that the current profile selections are displayed. See “Adding or Editing a Rights Assignment” on page 4-9.
- » To delete a row, click the trash can icon  at the far right of the row. This deletes the row from the table. A window appears giving you the opportunity to confirm or cancel the delete operation.
- » To reorder the rows in the table, use the up/down buttons  at the left of each row to move rows up or down in the table. The only row that cannot be moved is the bottom row. This “Any Identity—Any Connection—Unauthenticated Access” combination must always be left as the “fall-through” or default match for clients that do not match any other profile.

If the Rights Assignment Table contains more than 25 rows, the table will be displayed in pages of 25 rows. A set of page navigation controls are displayed at below the bottom right corner of the table. You can navigate among the pages in two ways:

- Use the forward and backward arrow buttons to view pages sequentially
- Select a page number from the drop-down list to go directly to a specific page

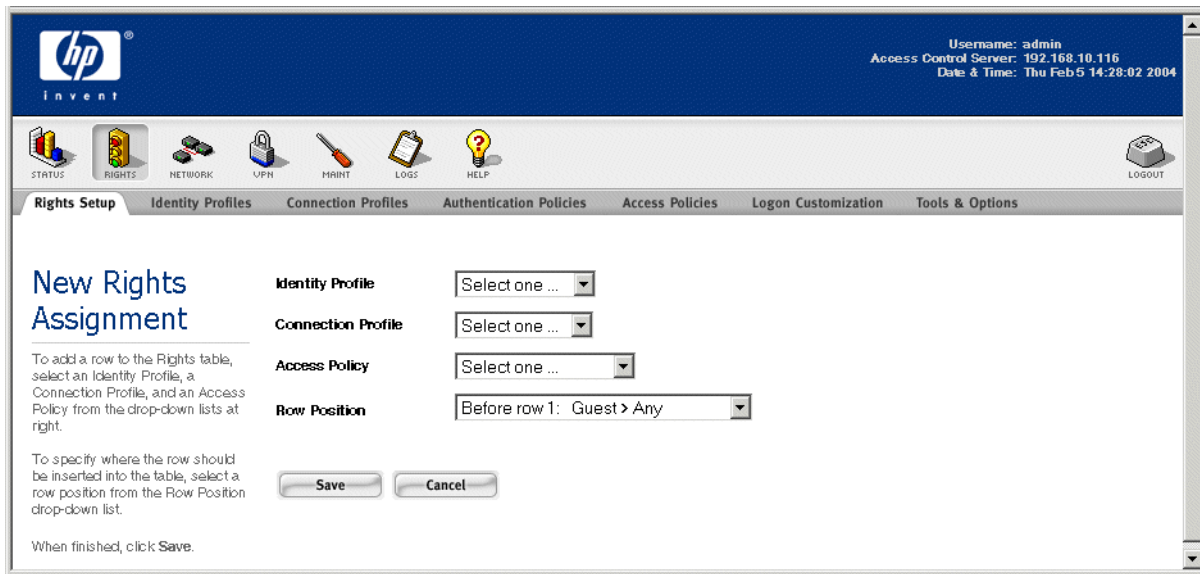
From the Rights Assignment Table you can also edit any of the Identity Profiles, Connection Profiles, or Access Policies shown in the table. To edit an individual profile or policy, click the name of the item you want to edit. The appropriate Edit page will be displayed.

Adding or Editing a Rights Assignment

To add a new row to the Rights Assignment Table, click the **New Rights Assignment...** button at the bottom of the table. The New Rights Assignment page appears, as shown in Figure 4-3, with the first three drop-down fields empty.

To edit a row, click the pencil icon at the end of the row. The Edit Rights Assignment page looks very similar to the New Rights Assignment page, but the fields are already filled in with the Identity Profile, Connection Profile, Access Policy, and row position of the Rights Assignment Table row to be edited. In addition, a **Save As Copy** button enables you to save a modified row definition without changing the original row.

Figure 4-3. The New Rights Assignment Page



Each field on this page contains a drop-down list from which you can select the components of a row in the Rights Assignment table, as defined in Table 4-1:

Table 4-1. New/Edit Rights Assignment Page Field Definitions

Field	Description
Identity Profile	A drop-down list of all Identity Profiles currently defined in the system. Pull down the list to select a profile. See "Identity Profiles" on page 4-11 for more information about defining Identity Profiles.
Connection Profile	A drop-down list of all Connection Profiles currently defined in the system. Pull down the list to select a profile. See "Connection Profiles" on page 4-29 for more information about defining Connection Profiles.
Access Policy	A drop-down list of all Access Policies currently defined in the system. Pull down the list to select a policy. See "Access Policies" on page 4-39 for more information about defining Access Policies.
Row Position	A drop-down list of the possible positions for the new row. The new row is inserted <i>ahead</i> of the row you select. Each row is identified by number as well as a summary of the Identity and Connection Profiles used. By default, the new row will be inserted at the top of the table (before row 1).

To create a new row for the Rights Assignment Table:

Step 1. Select an Identity Profile, a Connection Profile, and an Access Policy from the appropriate drop-down fields.

Step 2. Specify where in the table the new row should be placed. Order is important in matching a client to a row. The default position is to place the row at the top of the table.

Step 3. When you have made your selections, click **Save** to add this row to the table.

Cancel returns you to the previous page without saving any changes.

To edit an existing row, modify any of these fields to change the Identity Profile, Connection Profile, or the Access Policy, or to change the position of the row.

- » To replace the original row with the modified row definition, click **Save**.
- » To add the modified row as a new row, leaving the original row unchanged, click **Save As Copy**. (This button appears only on the Edit Rights Assignment page.)

After a **Save As Copy** you will stay on the same page so you can make additional changes.

Click **Cancel** to return to the previous page without making any further changes.

Note: *To have your changes affect currently connected clients, you must go to the Client Status page and refresh user rights. Otherwise, any changes you make take effect the next time a client gets new rights.*

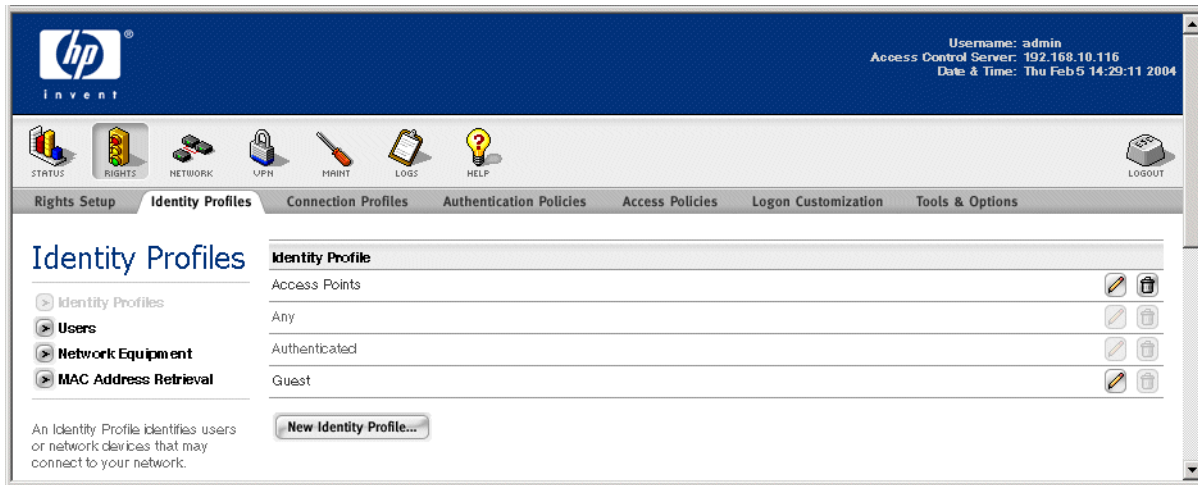
Identity Profiles

Identity Profiles represent named groups of users or equipment that have some characteristic in common—usually a common need for a certain set of access rights. An Identity Profile can be populated with user or network equipment entries from the built-in database, or it can represent an external group or domain. In the latter case, the Identity Profile does not need to have any specific Users or equipment associated with it. Instead, when a client is authenticated, a group or domain name is returned as part of the authentication process. If the returned group or domain information matches an Identity Profile name, the client is considered to be matched to that Identity Profile.

- » To view the current Identity Profiles, click the **Identity Profiles** tab visible at the top of any Rights Manager page.

The Identity Profiles page appears (see Figure 4-4).

Figure 4-4. The Identity Profiles Page



The 700wl Series system provides three predefined Identity Profiles, and a Rights Administrator can create additional ones. The predefined Identity Profiles can be considered default or implicit profiles, as users will match them automatically based on certain criteria.

The predefined Identity Profiles are:

- **Authenticated:** clients that have been successfully authenticated automatically match this profile
- **Guest:** clients that log on through the Guest logon feature automatically match this profile (Guests are not considered authenticated)
- **Access Points:** clients (identified by MAC address) that are actually Access Points
- **Any:** all clients automatically match this profile

These predefined profiles are typically used in rows at the bottom of the Rights Assignment Table, to catch clients that do not match more specific Identity Profiles higher in the table. If you plan to use these profiles in combination with other Identity Profiles you create, it is important that you order your rows correctly so that the more specific Identity Profile will be evaluated first.

- » To edit an Identity Profile, click the Identity Profile name in the first column of the table, or click the pencil icon at the end of the row. You cannot edit the Authenticated or Any profile.
- » To delete an Identity Profile, click the trash can icon at the end of the row. You cannot delete the predefined Identity Profiles.
- » To create a new Identity Profile, click the **New Identity Profile...** button at the bottom of the Identity Profiles list. This takes you to the New Identity Profile page

You can use the links directly under the page name in the left-hand panel of the page to go directly to the Users or Network Equipment pages to view lists of users and network equipment in the built-in database. You can also access the setup page to configure the automatic retrieval of MAC addresses from an LDAP database for inclusion in the built-in database. See “Users in the Built-In Database” on page 4-16, “Network Equipment in the Built-in Database” on page 4-20, or “Retrieving MAC Addresses from an LDAP Database” on page 4-24 for details on these functions.

Creating or Editing an Identity Profile

To create a new Identity Profile, click the **New Identity Profile...** button at the bottom of the Identity Profile list. The New Identity Profile page appears, as shown in Figure 4-5, with an empty Name field.

To edit an Identity Profile, click the Pencil icon at the end of the row. The Edit Identity Profile page is almost identical to the New Identity Profile page, except that the page displays the information about the Identity Profile you have selected. The name field is already filled in with the name of the Identity Profile you are editing. A **Save As Copy** button is also provided.

Figure 4-5. Creating a New Identity Profile

The screenshot shows the HP ProCurve Secure Access 700w Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the word 'invent'. The right side of the header displays the user's session information: Username: admin, Access Control Server: 192.168.10.116, and Date & Time: Thu Feb 5 14:29:38 2004. Below the header is a navigation menu with icons for STATUS, RIGHTS, NETWORK, VPN, PRINT, LOGS, HELP, and LOGOUT. The main content area is titled 'New Identity Profile' and contains the following fields and options:

- Name:** An empty text input field.
- Maximum Concurrent Logons Per User:** An empty text input field.
- Show all users and network equipment in the built-in database**
- Warning:** Unsaved changes will be lost if this is checked or unchecked. Displaying the built-in database may take a few minutes.
- Buttons:** Save and Cancel.

Below the main content area, there is a note: 'Provide a name for the Identity Profile. If the Identity Profile should match users that get a identity or domain name from an external authentication service, make sure its name is identical to the identity or domain name you want to match.'

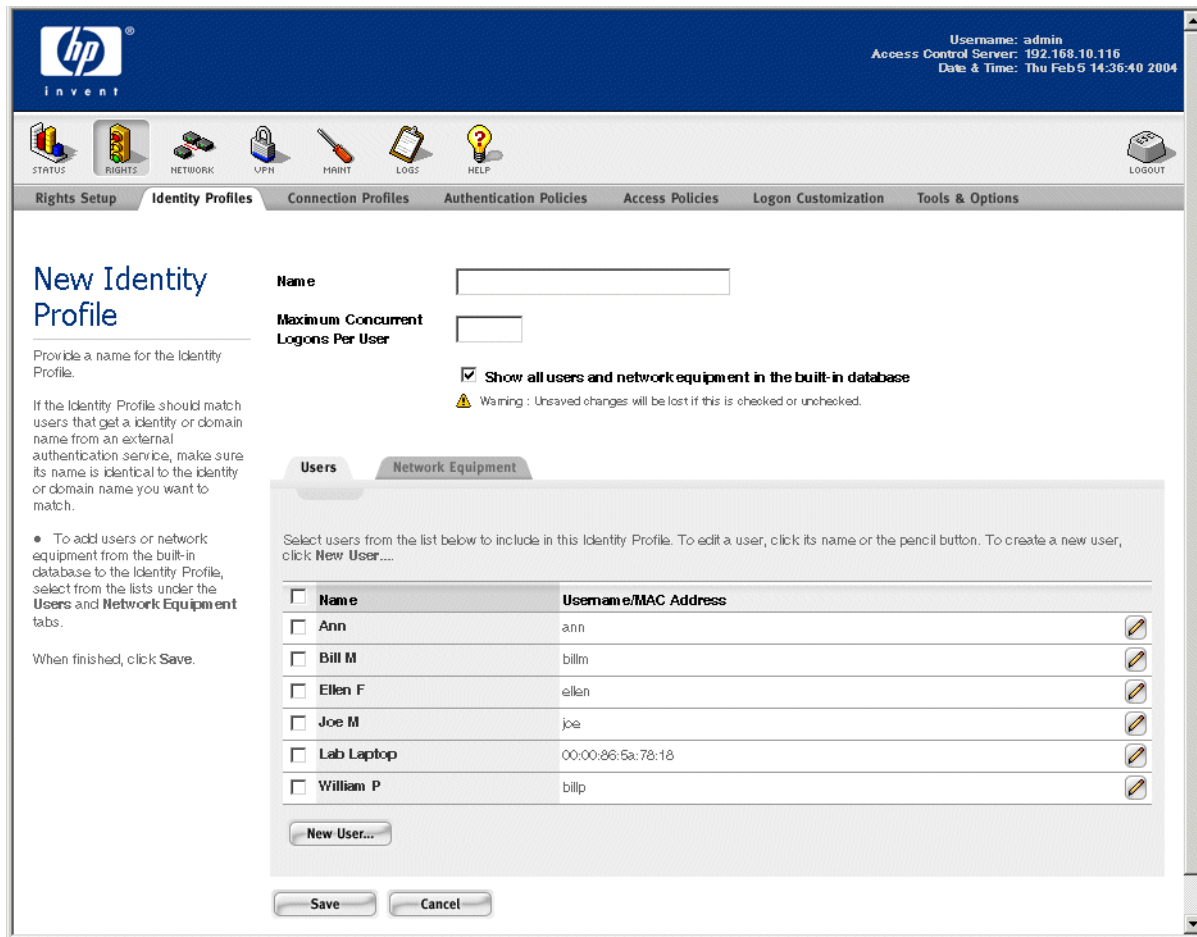
You have the option of displaying a list of the entries in the built-in database (Users or Network Equipment) but by default these are not displayed. If you are authenticating clients using an external authentication service you may not need to include users in the built-in database. On the other hand, if the database contains a large number of users (it can hold up to 5000 entries) the table of entries can take quite a while to paginate and display.

- » To show the list of Users or Network Equipment, check the **Show all users and network equipment in the built-in database** option, then click **Save**.

The New Identity Profile (or Edit Identity Profile) page is displayed again with the first page of the User tab showing (see Figure 4-6).

To display Network Equipment, select the Network Equipment tab.

Figure 4-6. Creating a New Identity Profile, with User list displayed



From this page, with the Users or Network Equipment list displayed, you can also add a new user or equipment item, or edit a user or equipment item. See “Users in the Built-In Database” on page 4-16 and “Network Equipment in the Built-in Database” on page 4-20 for details on these functions.

To create a new Identity Profile:

Step 1. Enter a name for the Identity Profile in the **Name** field.

If this Identity Profile is to be used to match an external group or domain, make sure the name matches exactly the group or domain you plan to match.

You can skip Step 3 if you are using this Identity Profile only to match an external group or domain.

Step 2. It is possible to limit the number of times a client can log on concurrently using the same username and password. To configure this feature, type a value in the **Maximum Concurrent Logons per User** field. A zero or blank is taken to mean “unlimited.”

If you allow multiple concurrent logons, then several clients can log on concurrently using the same username and password. This allows you to set up shared usernames such as for a kiosk application, or to allow users to log on through both wired and wireless connections simultaneously.

Limiting the number of logons per user does not prevent a user from logging on with that username and password—rather it prevents that user from matching this Identity Profile and thus getting rights based on matching this Identity Profile in the Rights Table. It is possible that the user could still get a set of rights based on matching a different Identity Profile.

When the concurrent logon limit is reached, the next client to log on using that username and password is still authenticated successfully, since the username and password are presumably still valid. The user will not match any rows in the Rights Table that use this Identity Profile, but could match a different Identity Profile and get rights based on that. For example, because this user could authenticate successfully, it will match the default “Authenticated” Identity Profile. If you have a row in your Rights table for the Authenticated Identity Profile, the user will get whatever rights are associated with that row.

- Step 3.** To include Users or Network Equipment from the built-in database in this Identity Profile:
- a. Check the **Show all users and network equipment in the built-in database** option and click **Save** to display the built-in database entries.
 - b. Click the **Users** or **Network Equipment** tab to display the appropriate list.
 - c. Click the checkboxes of the individual users or equipment items you want to include in this Identity Profile.

You can select the checkbox next to the **Name** column heading to select all items in the list. Clicking this checkbox a second time removes the checks from all items in the list.

Note: *You can skip this step if you are using this Identity Profile only to match an external group or domain.*

- Step 4.** Click **Save** to save this Identity Profile. If you are editing an existing Identity Profile, this replaces the original profile with the modified profile definition
- Cancel** returns you to the previous page without saving any changes.

To edit an existing Identity Profile:

- » To change the name of a profile, type a new name.
- » To add a user or equipment item (assuming the appropriate list is displayed) click its checkbox.
- » To remove a User or equipment item from the profile, click its checkbox again to remove the check. You can remove all users by clicking twice in the checkbox next to the Name column header.
- » To replace the original Identity Profile with the modified Identity Profile definition, click **Save**.
- » To add the modified Identity Profile as a new Identity Profile, leaving the original unchanged, click **Save As Copy**. This button appears only on the Edit Identity Profile page.

Click **Cancel** to return to the previous page without making any further changes.

Note: *To have your changes affect currently connected clients, you must go to the Client Status page and refresh user rights. Otherwise, any changes you make take effect the next time a client gets new rights.*

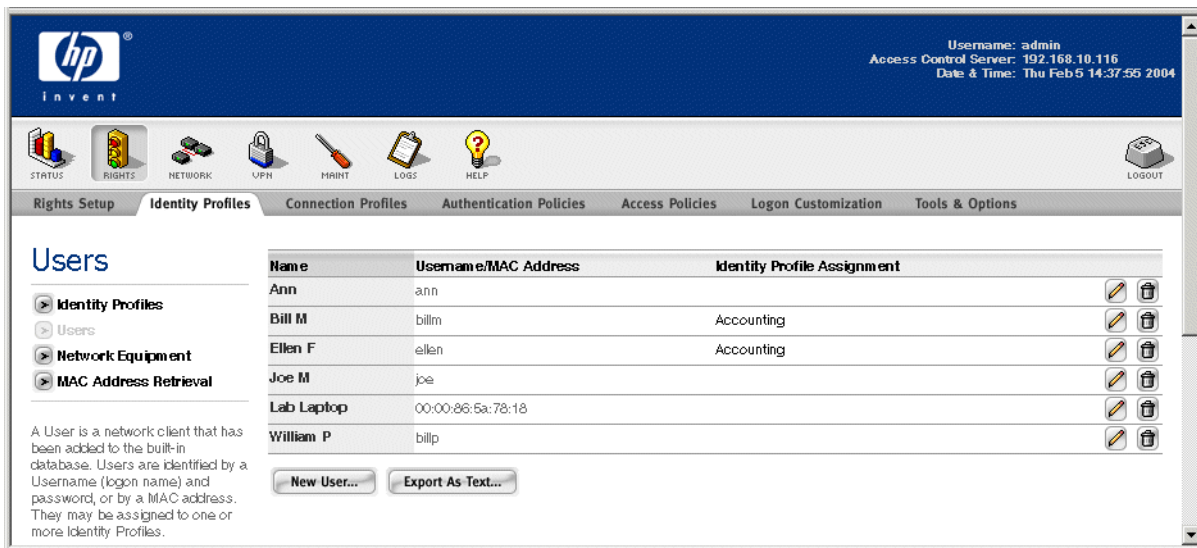
Users in the Built-In Database

Many organizations choose to authenticate their wireless users against a corporate database or authentication service. However, if you do not plan to use such a service, you can add users to the database built into the 700wl Series system and use that for authentication.

The built-in database can have other uses as well. If you want to pre-register Guest users, you can do so by adding them to the built-in database. You can also streamline the authentication process for selected users by adding them to the built-in database as MAC address users. This mechanism lets them bypass the normal external authentication process, and get the appropriate set of access rights immediately when they connect to the system. Finally, Administrator accounts are also kept in the built-in database.

- » To view the list of users currently defined in the built-in database, click the **Users** link from the Main Identity Profiles page.

Figure 4-7. Users in the Built-In Database



The current list of users is also displayed under the **Users** tab on the New Identity Profile or Edit Identity Profile screens, as shown in Figure 4-5.

The User list shows the following information about each user:

Table 4-2. Users Page Field Definitions

Field	Description
Name	The descriptive name for the user, that identifies the user in the 700wl Series system's Administrative Console.
Username/MAC Address	The user's logon ID or MAC address. A user may be identified by one or the other, not both.

Table 4-2. Users Page Field Definitions

Field	Description
Identity Profile Assignment	The Identity Profile to which the user has been assigned, if any. If no Identity Profile has been assigned, the user will automatically match either the “Authenticated” profile (if it has been authenticated) or the “Any” profile (if the user has not been authenticated—having not yet completed the logon process, or having bypassed authentication as a MAC address user).

- » To edit a user entry, click the user name in the Name column, or click the pencil icon at the end of the row. This takes you to the Edit User page to edit the entry for this user (see “Creating or Editing a User” on page 4-17).
- » To delete a user, click the trash can icon at the end of the row.
- » To create a new user entry, click the **New User...** button at the bottom of the User list. This takes you to the New User page (see “Creating or Editing a User”).
- » To export the entire list of users to file, use **Export as Text**. The list is displayed in a new browser window. Select **File->Save As** from the browser menu. The Save As dialog box appears. Select the file location and file type, type the file name and click **Save**.

From the Users page you can also go directly to the Identity Profiles page, the Network Equipment page, or the MAC Address Retrieval configuration page by clicking the link near the top of the left-hand column, just below the page name.

Creating or Editing a User

To create a new user, click **New User...** at the bottom of the Users list. The New User page appears, as shown in Figure 4-8, with empty fields and no Identity Profiles selected.

The Edit User page is almost identical to the New User page, except that fields are already filled in with the information about the user you have selected.

Configuring Rights

Figure 4-8. Adding a New User

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Console. The top navigation bar includes the HP logo, the word 'invent', and user information: Username: admin, Access Control Server: 192.168.10.116, Date & Time: Thu Feb 5 14:38:19 2004. Below the navigation bar are icons for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. The main content area is titled 'New User' and contains the following fields and sections:

- Name** (Descriptive Name): A text input field.
- Username / MAC Address**: A text input field with a checkbox for **MAC Address User**.
- Password**: A text input field.
- Confirm Password**: A text input field.
- Identity Profiles**: A section with a sub-header 'Identity Profiles' and a description: 'Assign this user to one or more Identity Profiles from the list below. To edit an Identity Profile, click its name or the pencil button. To add an Identity Profile, click **New Identity Profile...**'.
- Identity Profile List**: A table with columns for checkboxes, profile names, and edit buttons (pencil icons).

<input type="checkbox"/>	Identity Profile	
<input type="checkbox"/>	Guest (MAC address users may not be members of this Identity Profile)	
<input type="checkbox"/>	Access Points	
<input type="checkbox"/>	Accounting	
- New Identity Profile...**: A button.
- Save** and **Cancel**: Buttons at the bottom.

The fields on this page are as follows:

Table 4-3. New User Fields

Field	Description
Name	A descriptive name that identifies the user in the 700wl Series system's Administrative Console. This is the name that appears in Client Status display, among others. It can be the user's full name or any other meaningful name. This name may have up to 32 characters. Any 7-bit characters are allowed.

Table 4-3. New User Fields

Field	Description
Username/MAC Address	<p>The user's username (logon ID) or MAC address. A user may be identified by one or the other, not both.</p> <p>A username may have up to 50 characters. Any 7-bit characters are allowed.</p> <p>A MAC address can be entered with colons (:) or dashes (-) separating the tuples, or without any separation. Thus, 00:01:a2:b3:4c:d5, 00-01-a2-b3-4c-d5, and 0001a2b34cd5 are all valid formats for a MAC address.</p> <p>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:</p> <pre>00:05:A3:16:00:* 00:05:A3:16:0* 00:05:A3:* 0005A3* *</pre> <p>The wildcard character cannot be used in the middle of the string: 00:05:A3:*:00:02 is not a valid wildcard MAC address.</p>
MAC Address User	<p>Check this box to indicate that the contents of the previous field is a MAC address.</p> <p>You can use a MAC address rather than username to enable a client to get access rights without having to log in and be authenticated.</p>
Password	<p>The (optional) password associated with the user's logon name. This does not apply if a MAC address is provided rather than a username. The password may be up to 255 characters in length.</p>
Confirm Password	<p>The same password, entered a second time as a confirmation.</p>

To create a new user, do the following:

Step 1. Enter the identifying information about this user as defined in Table 4-3 above.

For users you want to authenticate using the built-in database, enter a username and password. These will be used to match against the username and password the user enters into the 700wl Series system's logon page.

If you want to bypass authentication, enter a MAC address instead of a username. In this case, as soon as the client connects to the system its MAC address is recognized as matching the MAC address in the built-in database. Assuming the MAC address has been assigned to an Identity Profile, that client will immediately get the rights defined by the Access Policy associated with the client's matching Identity Profile and Connection Profile.

Note: If you use wildcard MAC addresses, you must take care to ensure that the MAC address range you define does not include the MAC addresses of clients that you want to authenticate (i.e. to logon using a username and password). If a client's MAC address is recognized as matching within the MAC address range, that client will bypass the authentication process and will not have the opportunity to log on and provide a username. That client will then not match an Identity Profile based on its username, but rather will receive rights based on its MAC address.

Configuring Rights

Step 2. Select the Identity Profile to which this user should be assigned by clicking the appropriate checkbox in the Identity Profiles table.

As a rule, you would assign a user to only one Identity Profile, since the search for a match always stops at the first match found. Assigning a user to multiple Identity Profiles makes sense only if that user could connect through several different Connection Profiles, and thus could match different Identity Profile/Connection Profile combinations. This would be the case if you wanted to control a user's access based on his location or the time. For instance, you might want to give a user different access on weekends than he had during normal business hours.

To pre-register a user as a Registered Guest, assign the user to the Guest Identity Profile.

All clients authenticated with a username and password through the Built-in database are automatically associated with the "Authenticated" Identity Profile. If they do not match any other Identity Profile in the Rights table, they will get rights per the Access Policy associated with the Authenticated Identity Profile.

Note: Assigning a user to an Identity Profile is not sufficient to ensure that the user will get a specific set of rights; you must also make sure that the Identity Profile occurs in a position (row) in the Rights table such that the user will match the desired Identity Profile first, before matching some other Identity Profile such as the default Authenticated Identity Profile.

You can edit an Identity Profile by clicking its name or the pencil icon at the end of the row. To create a new Identity Profile, click the New **Identity Profile...** button at the bottom of the Identity Profiles table.

Note: If you do not explicitly associate a MAC address user with an Identity Profile, that client will continue to be associated with the "Any" Identity Profile, and will get rights (normally, just logon rights) on that basis. Because MAC Address users bypass the authentication process, they are NOT automatically associated with the default "Authenticated" Identity Profile.

Step 3. Click **Save** to save this User entry.

Cancel returns you to the previous page without saving any changes.

To edit an existing user entry, do the following:

- » Edit the fields to change the descriptive name, username, MAC address, password, or user type (admin level).
- » To change the Identity Profile to which the user is assigned, remove the check from the old Identity Profile and check the checkbox for the new Identity Profile.
- » When you have finished, click **Save**. This replaces the original user entry with the modified user information.

Click **Cancel** to return to the previous page without making any further changes.

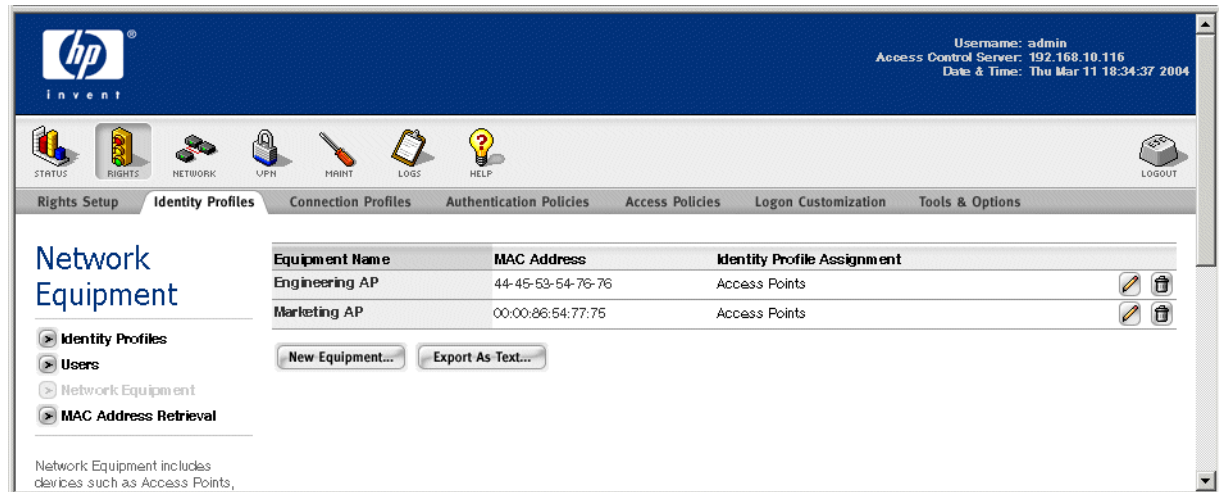
Network Equipment in the Built-in Database

Of the clients that connect to the 700wl Series system, some of them are network devices such as access points, hubs, or switches. For example, the Access Points connected through the downlink ports will appear as unauthenticated clients, identified by their MAC addresses, to the system. Access points and other network devices do not necessarily need to have access rights of their own in order to function

correctly in the system, however, if you want to manage these devices from within the 700wl Series system, you may want to assign them a specific set of access rights. You can add these devices to the built-in database and assign them to an Identity Profile so that they can get rights assigned through the Rights Assignment Table.

- » To view the list of network equipment currently defined in the built-in database, click the **Network Equipment** link from the main Identity Profiles page.

Figure 4-9. Network Equipment in the Built-In Database



The current list of network equipment is also displayed under the **Network Equipment** tab on the New Identity Profile or Edit Identity Profile screens, as shown in Figure 4-5.

The Network Equipment list shows the following information about each device:

Table 4-4. Network Equipment Page Field Definitions

Field	Description
Equipment Name	The descriptive name for the device
MAC Address	The MAC address of the network device.
Identity Profile Assignment	The Identity Profile to which the equipment has been assigned. (If no Identity Profile is assigned, the device will match the “Any” Identity Profile.)

- » To edit an equipment entry, click the user name in the Name column, or click the pencil icon at the end of the row. This takes you to the Edit Network Equipment page to edit the entry for this user (see “Creating or Editing an Equipment Entry” on page 4-22).
- » To delete an equipment entry, click the trash can icon at the end of the row.
- » To create a new equipment entry, click the **New Network Equipment...** button at the bottom of the Network Equipment list. This takes you to the New Network Equipment page (see “Creating or Editing an Equipment Entry”).
- » To export the Network Equipment list to file, use **Export as Text**. The list is displayed in a new browser window. Select **File->Save As** from the browser menu. The Save As dialog box appears. Select the file location and file type, type the file name and click **Save**.

Configuring Rights

From the Network Equipment page you can also go directly to the Identity Profiles page or to the Users page by clicking the link near the top of the left-hand column, just below the page name.

Creating or Editing an Equipment Entry



To create a new network equipment entry, click **New Network Equipment...** at the bottom of the Network Equipment list. The New Network Equipment page appears, as shown in Figure 4-8, with empty fields and no Identity Profile selected.

The Edit Network Equipment page is almost identical to the New Network Equipment page, except that fields are already filled in with the information about the equipment you have selected.

Figure 4-10. Adding a New Network Equipment Entry

The screenshot displays the HP InvenT web management interface. At the top, the HP logo and 'invent' text are on the left, and user information (Username: admin, Access Control Server: 192.168.10.116, Date & Time: Thu Feb 5 14:40:48 2004) is on the right. A navigation bar contains icons for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. Below this is a menu with tabs: Rights Setup, Identity Profiles (selected), Connection Profiles, Authentication Policies, Access Policies, Logon Customization, and Tools & Options.

The main content area is titled 'New Equipment'. It contains the following elements:

- Equipment Name:** A text input field.
- MAC Address:** A text input field.
- Identity Profiles:** A section with a sub-header 'Identity Profiles' and a description: 'Assign this equipment to one or more Identity Profiles from the list below. To edit an Identity Profile, click its name or the pencil button. To add an Identity Profile, click: **New Identity Profile...**'
- Identity Profile List:** A table with three rows:
 - Identity Profile**
 - Access Points 
 - Accounting 
- New Identity Profile...** button
- Save** and **Cancel** buttons at the bottom.

The fields on this page are as follows:

Table 4-5. New Network Equipment Fields

Field	Description
Name	A descriptive name for the device. This name may be up to 32 characters in length. Any 7-bit characters are allowed.
MAC Address	<p>The MAC address of the network device.</p> <p>A MAC address can be entered with colons (:) or dashes (-) separating the tuples, or without any separation. Thus, 00:01:a2:b3:4c:d5, 00-01-a2-b3-4c-d5, and 0001a2b34cd5 are all valid formats for a MAC address.</p> <p>A MAC address can be entered with colons (:) or dashes (-) separating the tuples, or without any separation. Thus, 00:01:a2:b3:4c:d5, 00-01-a2-b3-4c-d5, and 0001a2b34cd5 are all valid formats for a MAC address.</p> <p>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:</p> <pre>00:05:A3:16:00:* 00:05:A3:16:0* 00:05:A3:* 0005A3* *</pre> <p>The wildcard character cannot be used in the middle of the string: 00:05:A3:*:00:02 is not a valid wildcard MAC address.</p>

To create a new Network Equipment entry, do the following:

Step 1. Enter the identifying information about this equipment as defined in Table 4-3 above.

Note: *If you use wildcard MAC addresses, you must take care to ensure that the MAC address range you define does not include the MAC addresses of clients that you want to authenticate (i.e. to logon using a username and password). If a client's MAC address is recognized as matching within the MAC address range, that client will bypass the authentication process and will not have the opportunity to log on and provide a username. That client will then not match an Identity Profile based on its username, but rather will receive rights based on its MAC address.*

Step 2. Select the Identity Profile to which this network equipment should be assigned by clicking the appropriate checkbox in the Identity Profiles table.

Assign network equipment to only one Identity Profile, since the search for a match always stops at the first match found.

You can edit an Identity Profile by clicking its name or the pencil icon at the end of the row. To create a new Identity Profile, click the New **Identity Profile...** button at the bottom of the Identity Profiles table.

Step 3. Click **Save** to save this Network Equipment entry.

Cancel returns you to the previous page without saving any changes.

Configuring Rights

To edit a Network Equipment entry in the built-in database, do the following:

- » Edit the fields to change the descriptive name or the MAC address.
- » To change the Identity Profile to which the equipment is assigned, remove the check from the old Identity Profile and check the checkbox for the new Identity Profile to which this equipment should be assigned.
- » When you have finished, click **Save**. This replaces the original equipment entry with the modified information.

Click **Cancel** to return to the previous page without making any further changes.

Retrieving MAC Addresses from an LDAP Database

The 700wl Series system's built-in database can be used to keep the MAC addresses of Access Points and other client devices that cannot be authenticated using a user ID and password. If an organization has a large number of these types of clients, it may be impractical to add or update by hand the MAC addresses in the Network Equipment list of the built-in database. In addition, some organizations may already keep an inventory of such devices in an external database. The MAC Address Retrieval feature allows the built-in database to be populated and periodically updated with MAC address users 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 `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 an LDAP Service for MAC Address Retrieval

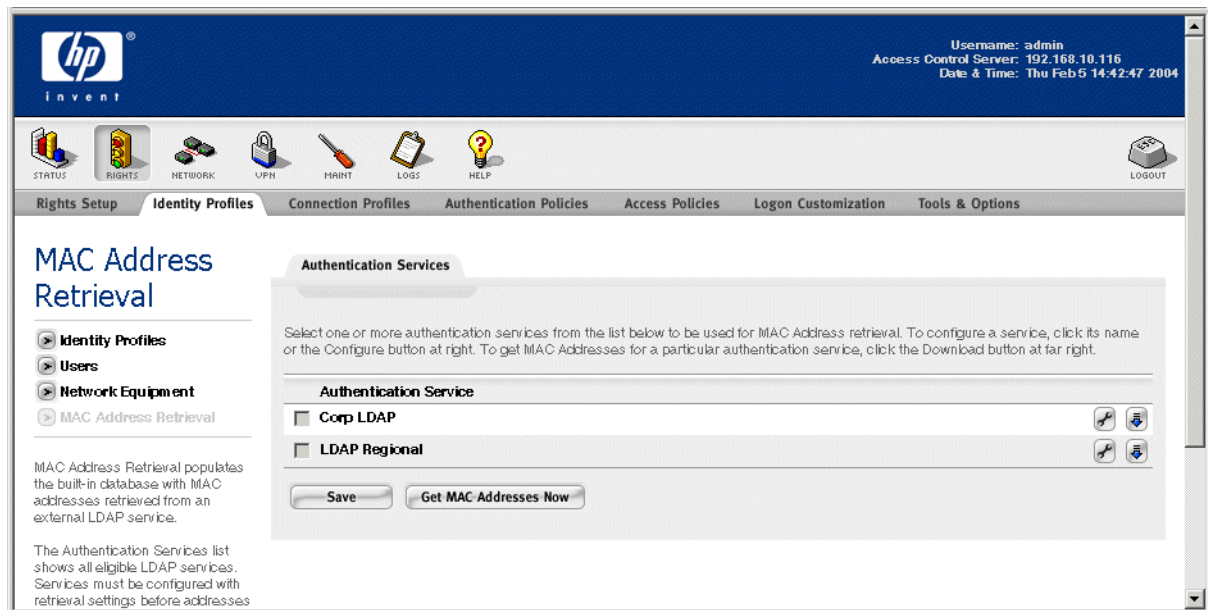
To set up MAC address retrieval from an LDAP service, do the following:

Step 1. From the main Identity Profiles page, click the **MAC Address Retrieval** link.

The MAC Address Retrieval page appears.

Figure 4-11 shows the MAC Address Retrieval page with several LDAP services that can be used for MAC address retrieval.



Figure 4-11. MAC Address Retrieval, Selecting an LDAP Service




If there are any LDAP services 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.

Configuring Rights

Note: If you have an LDAP service configured for user binding, that service does not appear in this list.

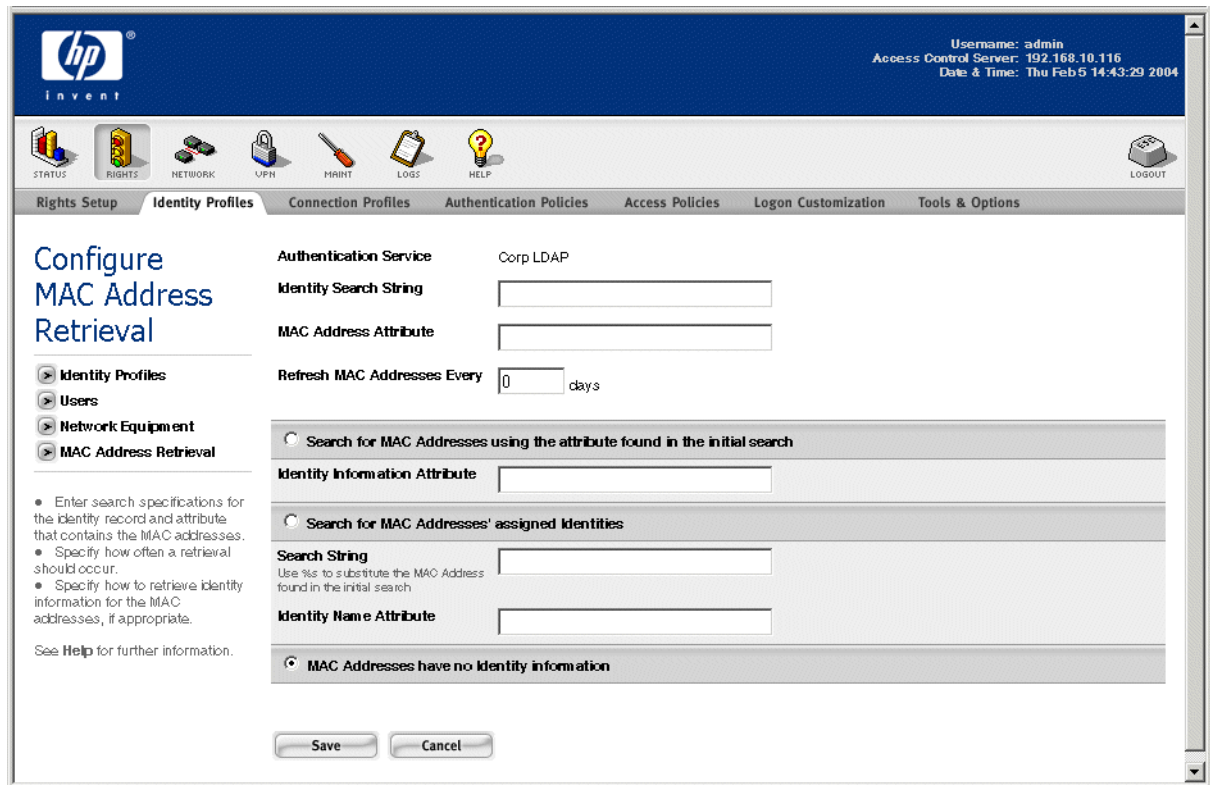
- » To configure or change the settings for MAC address retrieval, click the configuration icon  at the end of the row. You must configure the service for MAC address retrieval before you can enable it for retrieval.
- » To select an LDAP service to use as the source of MAC address users, click the checkbox next to the service name. The checkbox is enabled once you configure the service for MAC address retrieval.
- » To configure an LDAP service, or to modify a service configuration, see “Configuring Authentication Services” on page 5-7 in Chapter 5, “Configuring Authentication”.
- » To download MAC addresses from a specific LDAP database, click the download icon  at the end of the row. This does an immediate download from this individual database. You can do this even if you have configured MAC Address Retrieval to happen automatically at set intervals. If you have not configured the service for MAC address retrieval, attempting to download produces an error.
- » To immediately download addresses from all selected LDAP databases, click the **Get MAC Addresses Now** button. You can do this even if you have configured MAC Address Retrieval to happen automatically at set intervals.

Configuring the Search for MAC Addresses

To configure the MAC address retrieval parameters for an LDAP service, click the Configure icon  in the row for the service from which you want to retrieve MAC addresses.

The Configure MAC Address Retrieval page appears, as shown in Figure 4-12.

Figure 4-12. Configuring MAC Addresses Retrieval Parameters for an LDAP Service



The fields on this page are as follows:

Table 4-6. Configuring MAC Address Retrieval, address retrieval parameters

Field	Description
Authentication Service	The name of the LDAP service being configured.
Identity Search String	The search string that specifies the record in the database that contains the set of MAC addresses. For example, the search string <code>cn=MACS</code> specifies that the list of MAC address users can be found in a record whose <code>cn</code> is <code>MACS</code> .
MAC Address Attribute	The name of the attribute in the record that contains the individual MAC addresses, for example, <code>uniquemember</code> . Instances of this attribute should contain the MAC addresses that are to be added to the built-in database.
Refresh MAC addresses Every	The time interval (in days) between automatic refreshes of the MAC address data from the LDAP

If the MAC address users in your LDAP database do not have identity information kept in the database, you can save this configuration without specifying any further searches. In this case, when MAC addresses are retrieved, they will be added to the built-in database with no Identity Profile affiliation.

Configuring Rights

Identity Profile 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 identity 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 identity 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.

Table 4-7. MAC Address Retrieval, group identity retrieval parameters

Field	Description
Search for MAC Addresses using attribute found in initial search	Select this radio button to specify that the attribute entered in the Identity Information Attribute field below should be used as a search parameter when searching for MAC addresses.
Identity Information Attribute	If Search for MAC Addresses using attribute found in initial search is selected this field should contain the name of the attribute that contains the name(s) of the identity or identities.
Search for MAC Addresses' assigned identities	Select this radio button to specify that the string entered in the Search String field below should be used as a search parameter when searching for MAC addresses.
Search String	Search string to use to find records that contain the MAC address in a specified attribute. For example, the search string: (&(objectclass=groupofuniquenames) (uniquemember=%s)) searches records of class "groupofuniquenames" for an attribute "uniquemember" whose value matches the current MAC address as retrieved by the initial search.
Identity Name Attribute	Type the attribute name (for example, <code>cn</code>) who's value is the name of the group in which the matching <code>uniquemember</code> was found.
MAC Addresses have no identity information	Select this button to indicate that the MAC address users do not have identity information kept in the LDAP database. This is the default.

The following examples illustrate this in more detail.

Retrieving Group Identity 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, do the following:

Step 1. Select **Search for MAC Addresses using 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 **Identity Information Attribute**.

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 Identity Profile membership assumes that you have multiple group objects, each of which contains a list MAC address users. Identity Profile 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, do the following:

Step 1.Select **Search for MAC Addresses' assigned Identities**.

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 **Identity 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`.

Connection Profiles

A client is associated with a Connection Profile based on the Access Controller port through which he accesses the 700wl Series system, the VLAN to which he belongs (if any) and the day, date and time that he accesses the system. The default Connection Profile, "Any" includes clients from any Access Controller port, belonging to any VLAN or no VLAN, at any time, on any day.

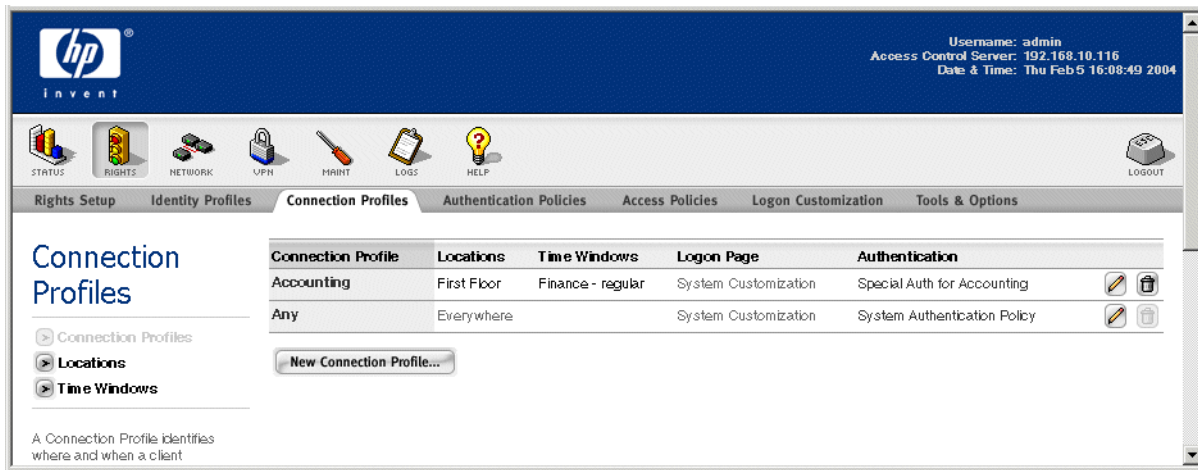
Configuring Rights

The Connection Profile is used in the Rights Assignment Table, in concert with the Identity Profile, to determine a client's access rights. If the client is unknown (i.e. has not been authenticated and does not match a known MAC address in the built-in database) the Connection Profile determines how to authenticate the client. This can include specification of a custom logon page as well as defining the Authentication Policy to use for authentication.

- » To view the currently defined Connection Profiles, click the **Connection Profiles** tab visible at the top of any Rights Manager page.

The Connection Profiles page appears (see Figure 4-13).

Figure 4-13. The Connection Profiles Page



The Connection Profiles table displays the following information about each Connection Profile:

Table 4-8. Connection Profiles Table Contents

Column	Description
Connection Profile	The name of the Connection Profile
Locations	The Locations included in this Connection Profile. A Connection Profile can include multiple Locations. A Location defines a set of Access Controller ports to be included in this Connection Profile. See "Locations" on page 4-35 for information about defining a Location.
Time Windows	The Time Windows included in this Connection Profile. A Connection Profile can include multiple Time Windows. A Time Window defines a time period during which this Connection Profile is available as a valid match for a client. See "Time Windows" on page 4-37 for more information about defining Time Windows.
Logon Page	The Logon page that should be presented to an unknown client that matches this Connection Profile, if the Authentication Policy associated with this Connection Profile uses a browser-based logon page.
Authentication	The Authentication Policy that applies to unknown clients that match this Connection Profile. See "Authentication Policies" on page 5-4 for more information about defining Authentication Policies.

- » To edit a Connection Profile, click the Connection Profile name in the first column of the table, or click the pencil icon at the end of the row. This takes you directly to the Edit Connection Profile page (see “Creating or Editing a Connection Profile” on page 4-31).
- » To delete a Connection Profile, click the trash can icon at the end of the row.

Note: You cannot delete a Connection Profile that is in use—an error message will inform you if this is the case. You must first remove the Connection Profile from use in any rows in the Rights Assignment Table.

- » To create a new Connection Profile, click the **New Connection Profile...** button at the bottom of the Connection Profiles list. This takes you to the New Connection Profile page.

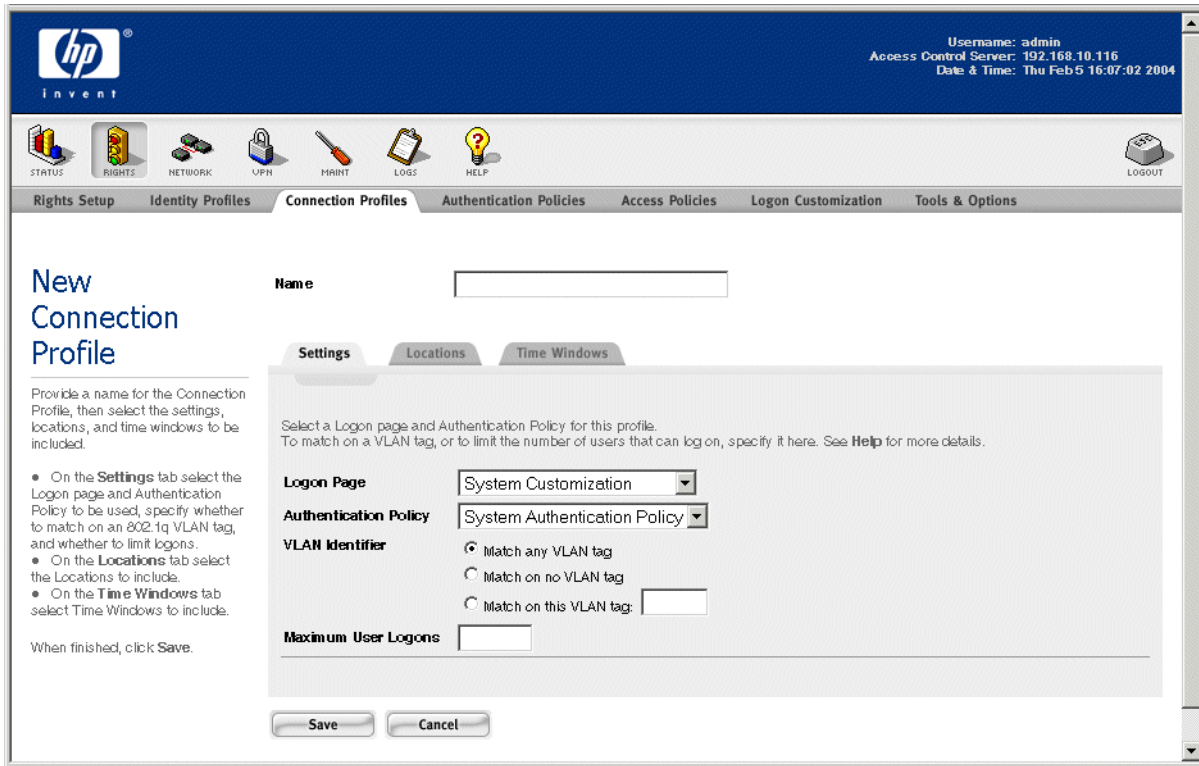
From the Connection Profiles page you can go directly to the Locations or Time Windows pages using the links directly under the page name in the left-hand panel of the page.

Creating or Editing a Connection Profile

To create a new Connection Profile, click the **New Connection Profile...** button at the bottom of the list on the Connection Profiles page. The New Connection Profile page appears (see Figure 4-14), with the **Settings** tab initially displayed.

The Edit Connection Profile page is almost identical to the New Connection Profile page, except that the page displays the information about the Connection Profile you have selected. The name field is already filled in with the name of the Connection Profile you are editing, and the fields under the Settings tab are filled in with the settings for this Connection Profile. The Locations and Time Windows lists display checkboxes that indicate the Locations and Time Windows that have been included in this Connection Profile.

Figure 4-14. Creating a New Connection Profile, the Settings Tab



To create or edit a Connection Profile, do the following:

Step 1. Type a name for a new Connection Profile. You can change the name of an existing Connection Profile by typing a new name.

Step 2. On the **Settings** tab, select or enter data into the fields as described in Table 4-9 below.

The fields under the **Settings** tab are as follows:

Table 4-9. New Connection Profile Settings Tab Contents

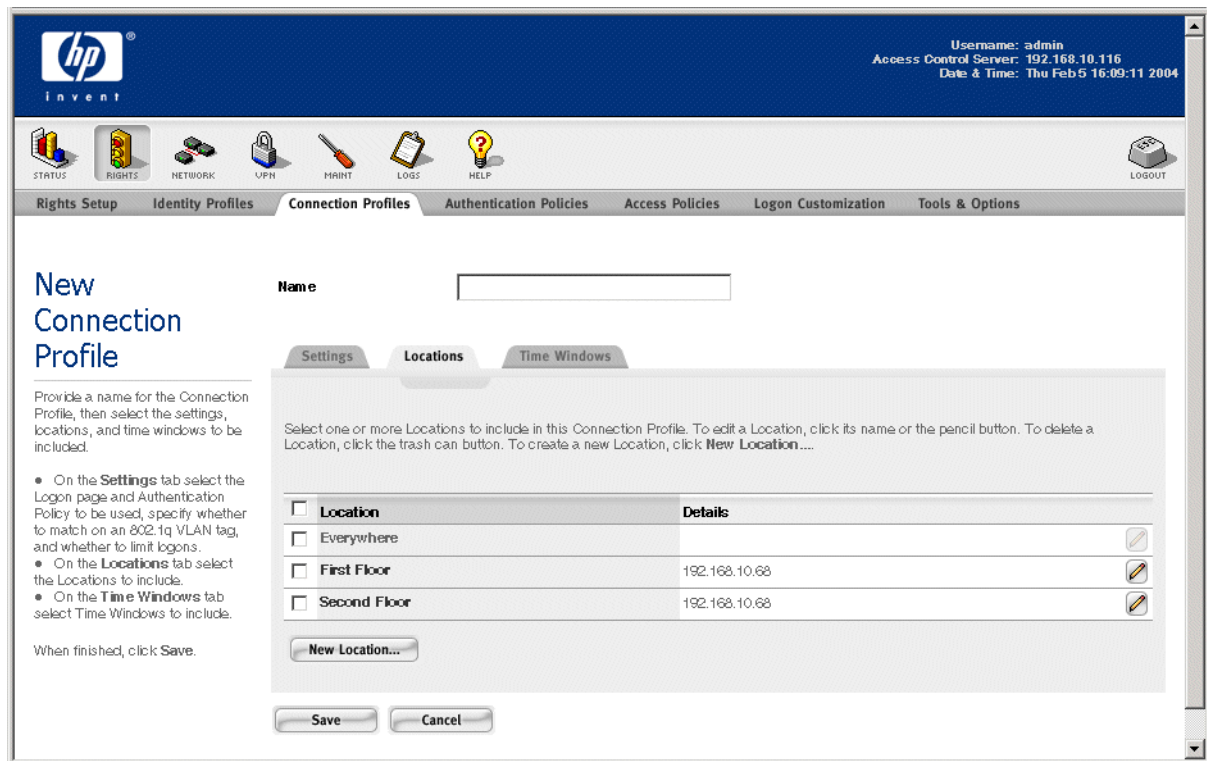
Column	Description
Logon Page	The Logon page that should be presented to an unknown client that matches this Connection Profile, if the Authentication Policy associated with this Connection Profile uses a browser-based logon page. This setting lets you specify a custom Logon page for this Connection Profile. You can select from a list of custom Logon pages currently defined within the 700wl Series system. See “ Logon Page Customization ” in Chapter 5 on page 5-30 for more information on creating custom Logon pages.
Authentication Policy	The Authentication Policy that should be used to authenticate unknown clients that match this Connection Profile. You can select from a list of Authentication Policies defined within the 700wl Series system. See “ Authentication Policies ” in Chapter 5 on page 5-4 for more information about Authentication Policies.

Table 4-9. New Connection Profile Settings Tab Contents (Continued)

Column	Description
VLAN Identifier	<p>How an 802.1Q VLAN Identifier (tag) should be used to determine whether a client matches this Connection Profile:</p> <ul style="list-style-type: none"> • Select Match any VLAN tag if clients should always match this Connection Profile regardless of any VLAN tags associated with packets from those clients • Select Match on no VLAN tag if only clients sending untagged packets should match this Connection Profile. • Select Match on this VLAN tag (and enter the tag) if only clients sending packets with the specified tag should match this Connection Profile.
Maximum User Logons	<p>The maximum number of clients that are allowed to log on to the 700w Series system under this Connection Profile. The default is unlimited.</p> <p>Note: <i>If multiple Connection Profiles include the same Location, then the number of clients allowed to log on through that Location will be the sum of the Maximum User Logons allowed for all Connection Profiles that include the Location.</i></p>

Step 3. On the **Locations** tab, as shown in Figure 4-15, select one or more Locations that should be included in this Connection Profile.

Figure 4-15. Creating a Connection Profile, the Locations Tab



Configuring Rights

The Locations tab shows a list of the currently defined Locations. The columns in this list are as follows:

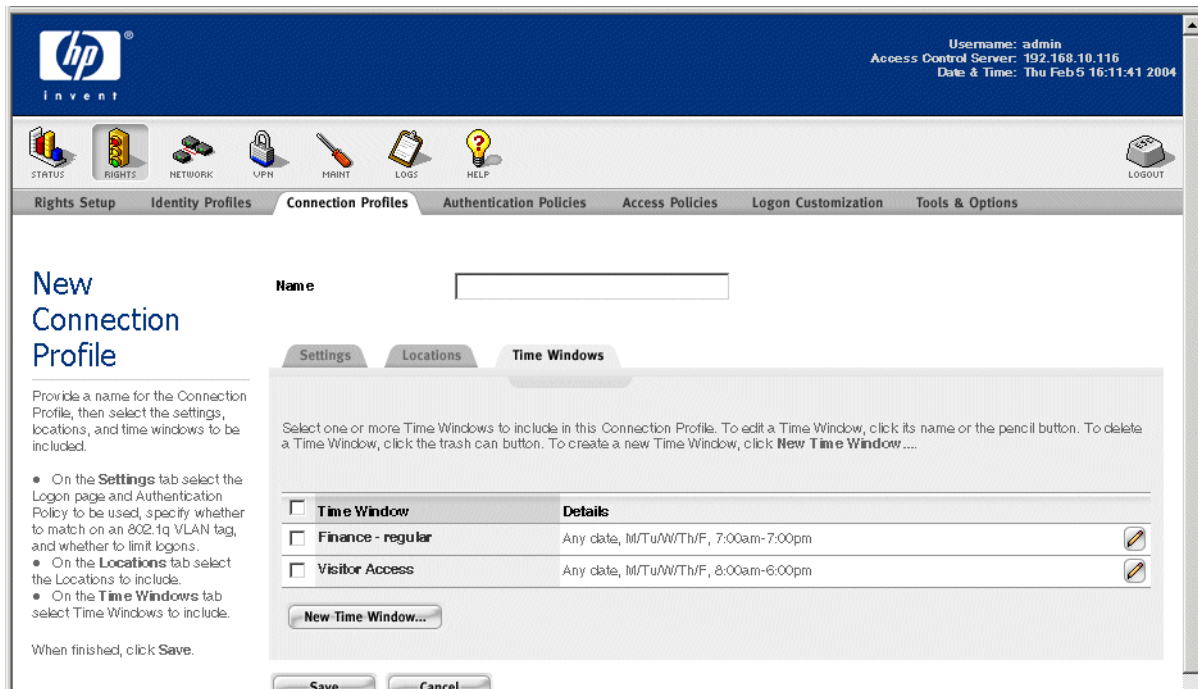
Table 4-10. Locations Tab Column Definitions

Column	Description
Name	The descriptive name for the Location.
Details	The definition of the Access Controllers and ports included in the Location.

- To select all Locations in the list, select the checkbox next to the Locations column heading. Clicking this checkbox a second time removes the checks from all Locations in the list.
- To remove a Location from the profile, click its checkbox to remove the check.

Step 4. On the **Time Windows** tab, as shown in Figure 4-16, select the Time Windows to include in this Connection Profile.

Figure 4-16. Creating a Connection Profile, the Time Windows Tab



The Time Windows tab shows a list of the currently defined Time Windows. The columns in this list are as follows:

Table 4-11. Time Windows Tab Column Definitions

Column	Description
Time Window	The descriptive name for the Time Window.
Details	The definition of the Time Window.

- To select all Time Windows in the list, select the checkbox next to the Locations column heading. Clicking this checkbox a second time removes the checks from all Time Windows in the list.
- To remove a Time Window from the profile, click its checkbox to remove the check.

Step 5. Click **Save** to save this Connection Profile. If you are editing a Connection Profile, this replaces the original Connection Profile with the modified Connection Profile definition.

To add the modified Connection Profile as a new Connection Profile, leaving the original Connection Profile unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Connection Profile page.

The page remains displayed so you can make additional changes.

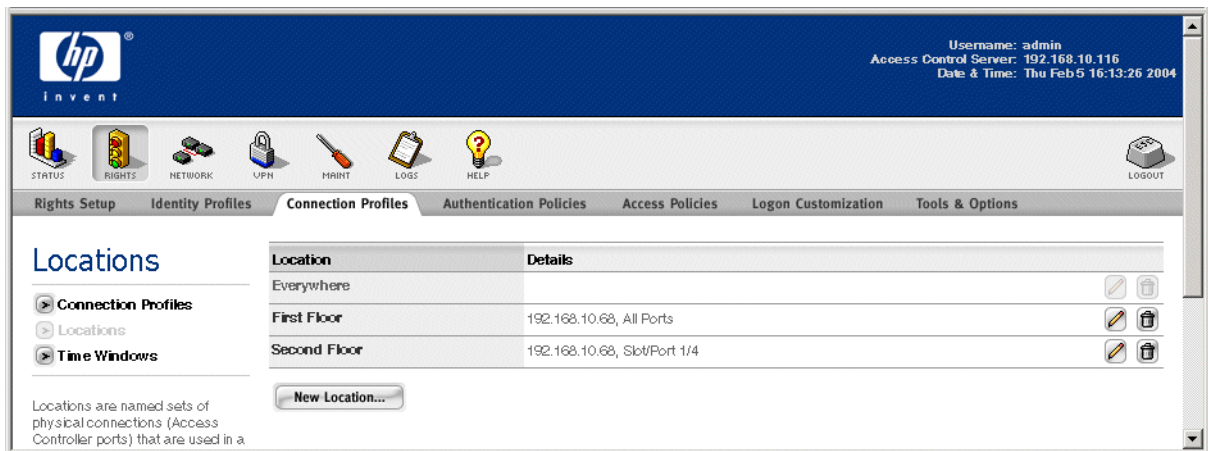
Click **Cancel** to return to the previous page without making any further changes.

Locations

A Location is a named set of physical connections (Access Controller ports) into the 700wl Series system. A Location can include all ports on the Access Controller, or it can include just a single port.

- » To view the list of Locations currently defined in the 700wl Series system, click the **Locations** link on the main Connection Profiles page. The Locations page appears, as shown in Figure 4-17.

Figure 4-17. Locations List



The Location list shows the following information about each Location:

Table 4-12. Locations Page Field Definitions

Field	Description
Name	The descriptive name for the Location.
Details	The definition of the Access Controllers and ports included in the Location.

- » To edit Location, click the Location name in the Name column, or click the pencil icon at the end of the row. This takes you directly to the Edit Location page to edit the entry for this user (see “Creating or Editing a Location” on page 4-36).

Configuring Rights

- » To delete a Location, click the trash can icon at the end of the row.
- » To create a new Location, click the New Location... button at the bottom of the Locations list. This takes you to the New Location page (see “Creating or Editing a Location”).

From this page you can also go directly to the Connection Profiles or Time Windows pages using the links directly under the page name in the left-hand panel of the page. See “Connection Profiles” on page 4-29 and “Time Windows” on page 4-37 for details on these functions.

Creating or Editing a Location

To create a new Location, click **New Location...** at the bottom of the Location list. The New Location page appears, as shown in Figure 4-18, displaying a list of all Access Controllers known to the Access Control Server, which a list of the ports that exist on each Access Controller.

The Edit Location page is almost identical to the New Location page, except that the name and the port selections are displayed for the Location you have selected.

Figure 4-18. Adding a New Location

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes the HP logo and the text 'invent'. The user is logged in as 'admin' with the Access Control Server IP '192.168.10.116' and the date/time 'Thu Feb 5 16:13:59 2004'. The main navigation bar has tabs for 'Rights Setup', 'Identity Profiles', 'Connection Profiles', 'Authentication Policies', 'Access Policies', 'Logon Customization', and 'Tools & Options'. The 'New Location' page is displayed, featuring a form with the following fields: 'Name' (text input), 'Access Controller' (dropdown menu showing '192.168.10.68'), and 'Slot/Port' (dropdown menu showing 'All Ports'). Below the form are 'Save' and 'Cancel' buttons. A note at the bottom of the form reads: 'When finished, click Save.'

To create or edit a Location, do the following:

- Step 1.** Type a name for this Location. You can change the name of an existing Location by typing a new name.
- Step 2.** Select the ports on the Access Controllers that should be included in this Location.
- Step 3.** Click **Save** to save this Location. If you are editing the Location, this replaces the original Location with the modified Location definition.

To add a modified Location as a new Location, leaving the original Location unchanged, click **Save As Copy**. The **Save As Copy** button appears only on the Edit Location page.

After a **Save As Copy** the page remains displayed so you can make additional changes.

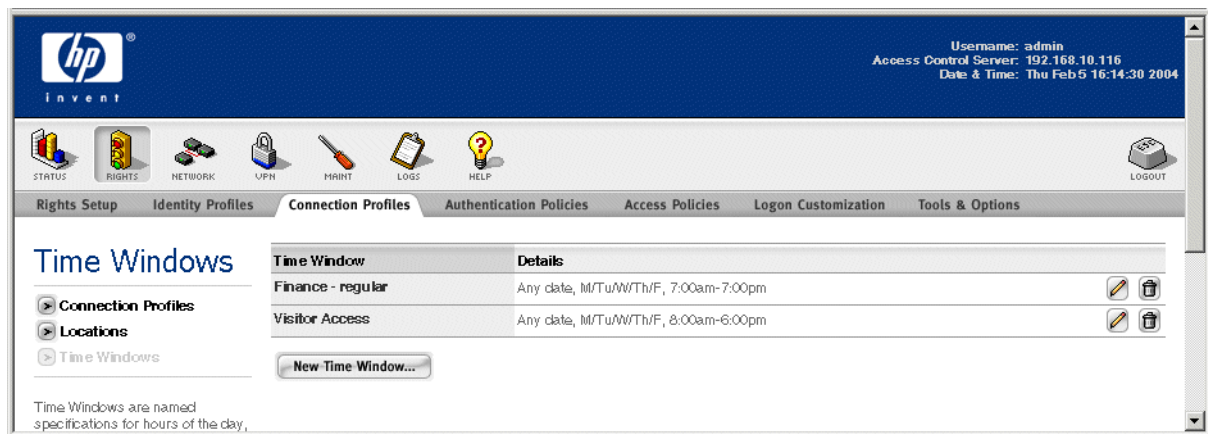
Click **Cancel** to return to the previous page without making any further changes.

Time Windows

A Time Window is a specification of a period of time, defined by specific dates or date ranges, days of the week, and hours of the day. Time Windows may be used to limit when a Connection Profile is available as a valid match for a client. If a client connects to the 700wl Series system through a port included in the Connection Profile, but the time of the connection is not within the Time Window(s) specified for the Connection Profile, then the client will not match that Connection Profile.

- » To view the list of Time Windows currently defined in the 700wl Series system, click the **Time Windows** link on the main Connection Profiles page. The Time Windows page appears, as shown in Figure 4-17.

Figure 4-19. The Time Windows List



The Time Window list shows the following information about each Time Window:

Table 4-13. Time Windows List Column Definitions

Column	Description
Time Window	The descriptive name for the Window.
Details	The definition of the Time Window.

- » To edit Time Window, click the Time Window name in the Time Window column, or click the pencil icon at the end of the row. This takes you directly to the Edit Time Window page to edit the entry for this user (see “Creating or Editing a Time Window” on page 4-38).
- » To delete a Time Window, click the trash can icon at the end of the row.
- » To create a new Time Window, click the **New Time Window...** button at the bottom of the Time Windows list. This takes you to the New Time Window page (see “Creating or Editing a Time Window”).

From this page you can also go directly to the Connection Profiles or Locations pages using the links directly under the page name in the left-hand panel of the page. See “Connection Profiles” on page 4-29 and “Locations” on page 4-35 for details on these functions.

Creating or Editing a Time Window

To create a new Time Window, click **New Time Window...** at the bottom of the Time Window list. The New Time Window page appears, as shown in Figure 4-18, with a blank name field and default time settings.

The Edit Time Window page is almost identical to the New Time Window page, except that the name and port selections are displayed for the Time Window you have selected, and a **Save As Copy** button is available.

Figure 4-20. Adding a New Time Window

To create or edit a Time Window, do the following:

Step 1. Type a name for this Time Window in the **Name** field. You can change the name of an existing Time Window by typing a new name.

Step 2. Select the Time Window specification using the settings described in Table 4-14 below.

The Time Window settings you can select are as follows:

Table 4-14. New Time Window Settings

Setting	Description
Valid Dates	Specify a Time Window by calendar dates: <ul style="list-style-type: none"> • The default is Any date • To specify a range of dates, click the From radio button and then select the beginning and ending dates using the drop-down fields. To specify a single date, select the same value for both the beginning and ending dates.

Table 4-14. New Time Window Settings

Setting	Description
Valid Days	Specify a Time Window by days of the week: <ul style="list-style-type: none"> The default is Any day To specify particular days, click the Selected days radio button, then check the individual days of the week you want to include.
Valid Times	Specify a Time Window by hours of the day: <ul style="list-style-type: none"> The default is Any time To specify a range of time, click the From radio button and then select the beginning and ending times using the drop-down fields. You can specify the range in 5-minute increments.

You can combine all three settings to create a specific Time Window. For example, you could specify a Time Window that's valid on Mondays, Wednesdays, and Fridays from 11:00 am until 2:00 pm, between June 1, 2003 and September 15, 2003.

Step 3. Click **Save** to save this Time Window. If you are editing an existing Time Window, this replaces the original Time Window with the modified Time Window definition.

To add the modified Time Window as a new Time Window, leaving the original Time Window unchanged, click **Save As Copy**. The **Save As Copy** button appears only on the Edit Location page.

After a **Save As Copy** the page remains displayed so you can make additional changes.

Click **Cancel** to return to the previous page without making any further changes.

Access Policies

Access Policies define many aspects of how a client interacts with the network. An Access Policy may be used to define the following properties of a client session:

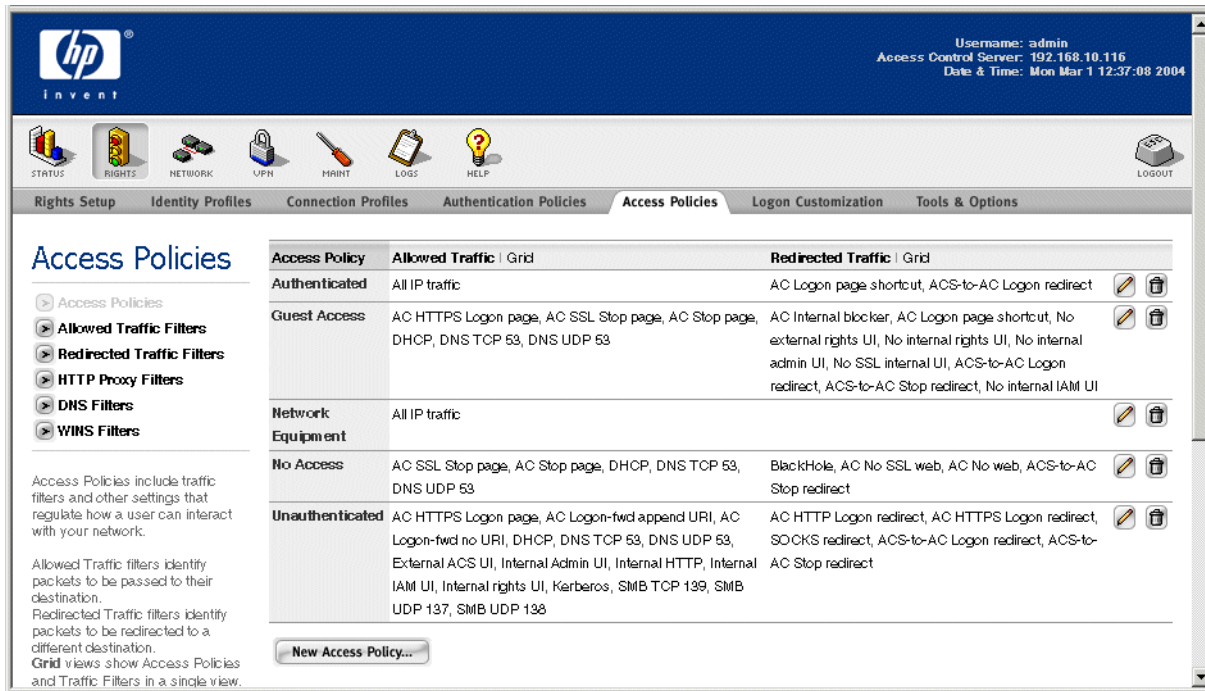
- Which packets are allowed to be passed on to their destinations, which packets will be redirected to alternate destinations, and which will be dropped
- How client IP addressing is handled—whether clients can use static IP addresses, real IP addresses via DHCP, or whether they will be NAT'ed
- What type of encryption is allowed or required, if any
- HTTP proxy filters that specify what web sites are accessible or restricted
- Bandwidth limits for traffic to and from the client
- Timeout values for a valid authentication—the time interval after which a client will be forced to reauthenticate

A client is associated with an Access Policy based on the Identity Profile and Connection Profile that it matches at any point in time.

- » To view the current Access Policies, click the **Access Policies** tab visible at the top of any Rights Manager page.

The Access Policies page appears (see Figure 4-21).

Figure 4-21. The Access Policies Page



The 700wl Series system provides five predefined Access Policies, and a Rights Administrator can create additional ones. The predefined Access Policies are:

- **Authenticated:** This defines a default set of rights for users that have been successfully authenticated.
- **Guest Access:** This defines a default set of rights for users that have logged on using the “Logon as a Guest” feature.
- **Network Equipment:** This defines a default set of rights appropriate for network devices such as Access Points, hubs, switches and so on.
- **No Access:** This defines a default set of rights that may be used to deny all access to a client.
- **Unauthenticated:** This defines a default set of rights for users that are not recognized by the 700wl Series system. These rights by default allow a user to access only the 700wl Series system logon page.

You may use these Access Policies as they are, modify them, or use them as the basis for new Access Policies.

The Access Policies table displays the following information about each Access Policy:

Table 4-15. Access Policies Table Contents

Column	Description
Access Policy	The name of the Access Policy

Table 4-15. Access Policies Table Contents

Column	Description
Allowed Traffic Grid	<p>A list of the Allowed Traffic Filters selected for the Access Policy.</p> <p>Click Grid in the column heading to display all Access Policies and Allowed Traffic Filters in a grid format. See “The Allowed Traffic Filters Grid” below for an explanation of that display format.</p> <p>See “Creating or Editing an Allowed Traffic Filter” on page 4-64 for information about defining Allowed Traffic Filters.</p>
Redirected Traffic Grid	<p>A list of the Redirected Traffic Filters selected for Access Policy.</p> <p>Click Grid in the column heading to display all Access Policies and Redirected Traffic Filters in a grid format. See “The Redirected Traffic Filters Grid” on page 4-42 for an explanation of that display format.</p> <p>See “Creating or Editing a Redirected Traffic Filter” on page 4-67 for information about defining Allowed Traffic Filters.</p>

- » To edit an Access Policy, click the Access Policy name in the first column of the table, or click the pencil icon at the end of the row. This takes you directly to the Edit Access Policy page (see “Creating or Editing an Access Policy” on page 4-43).
- » To edit an Allowed Traffic Filter or a Redirected Traffic Filter, click the name of the filter you want to edit. This takes you directly to the Edit Filter page for the filter you selected.
- » To delete an Access Policy, click the trash can icon at the end of the row.

Note: You cannot delete an Access Policy that is in use—an error message will inform you if this is the case. You must remove the Access Policy from all rows in the Rights Assignment Table before you can delete that policy.

- » To create a new Access Policy, click the **New Access Policy...** button at the bottom of the Access Policies list. This takes you to the New Access Policies page.
- » To view the list of all Allowed Traffic Filters or Redirected Traffic filters, click the links directly under the page name in the left-hand panel of the page.

Viewing Filters—the Grid Views

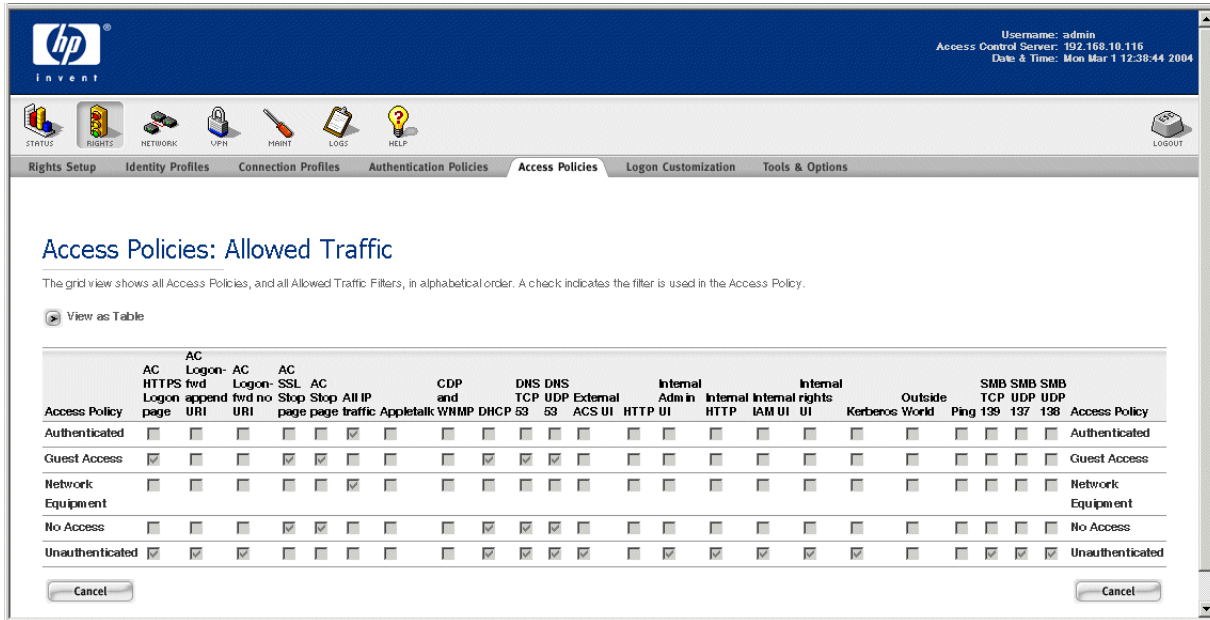
The Grid view format allows you to view all Access Policies and display all the Allowed Traffic Filters or all Redirected Traffic Filters in a single table view. This format makes it easy to compare the filters that are enabled or disabled between different Access Policies.

The Allowed Traffic Filters Grid

The Allowed Traffic Filters Grid displays all Access Policies and Allowed Traffic Filters in a grid layout, as shown in Figure 4-22.

Configuring Rights

Figure 4-22. Access Policies and Allowed Traffic Filters in a Grid Format



Each row represents an Access Policy. The Allowed Traffic Filters are shown in columns. Filters that are enabled for the Access Policy are represented by checks in the appropriate column checkbox. This format makes it easy to compare which filters are enabled for different Access Policies.

- » To edit an Access Policy, click the Access Policy name. This takes you directly to the Edit Access Policy page for that policy.
- » To edit an Allowed Traffic Filter, click the filter name. This takes you directly to the Edit Filter page for the filter you selected.
- » Click **Cancel** to return to the previous page without making any changes.
- » To return to the table layout, click the **View As Table** link above the left corner of the grid.

The Redirected Traffic Filters Grid

The Redirected Traffic Filters Grid displays all Access Policies and Redirected Traffic Filters in a grid layout, as shown in Figure 4-23.

Figure 4-23. Access Policies and Redirected Traffic Filters in a Grid Format

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The main content area is titled "Access Policies: Redirected Traffic". Below the title, there is a "View as Table" link. The table below lists various Access Policies and their associated Redirected Traffic Filters, with checkboxes indicating which filters are enabled for each policy.

Access Policy	AC HTTP Logon	AC HTTPS Logon	AC AC redirect	AC Logon internal page	AC No SSL shortcut	AC No web	ACS- to-AC Logon redirect	ACS- to-AC Stop redirect	No external rights UI	No internal admin UI	No internal IAM UI	No internal rights UI	No internal SSL redirect	SOCKS	Access Policy
Authenticated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Authenticated
Guest Access	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Guest Access
Network Equipment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Network Equipment
No Access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	No Access
Unauthenticated	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Unauthenticated

Each row represents an Access Policy. The Redirected Traffic Filters are shown in columns. Filters that are enabled for the Access Policy are represented by checks in the appropriate column checkbox. This format makes it easy to compare which filters are enabled for different Access Policies.

Note: Because each Access Policy may order the precedence of Redirected Traffic Filters differently, it is not possible to reflect that ordering correctly for all Access Policies in this format. Therefore, the Redirect filters in this grid are displayed in alphabetical order. In order to determine the precedence of Redirected Traffic Filters for an individual Access Policy, you must view that Access Policy.

- » To edit an Access Policy, click the Access Policy name. This takes you directly to the Edit Access Policy page for that policy.
- » To edit a Redirected Traffic filter, click the filter name. This takes you directly to the Edit Filter page for the filter you selected.
- » Click **Cancel** to return to the previous page without making any changes.
- » To return to the table layout, click the **View As Table** link above the left corner of the grid.

Creating or Editing an Access Policy

To create a new Access Policy, click the **New Access Policy...** button at the bottom of the list on the Access Policies page. The New Access Policy page appears (see Figure 4-24) with the **Settings** tab initially displayed.

The Edit Access Policy page is almost identical to the New Access Policy page, except that the name and settings are displayed for the Access Policy you have selected. Also, a **Save As Copy** button is provided.

Figure 4-24. Creating a New Access Policy, the Settings Tab

The screenshot shows the HP ProCurve management interface. At the top, there is a navigation bar with icons for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. Below this is a menu bar with tabs for Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies (selected), Logon Customization, and Tools & Options. The main content area is titled 'New Access Policy' and contains a 'Name' field. Below the name field are several tabs: Settings (selected), Allowed Traffic, Redirected Traffic, HTTP Proxy, Bandwidth, and Timeout. The 'Settings' tab is active, showing configuration options for Network Address Translation (set to 'Always'), IP Addressing (set to 'Require DHCP'), VLAN Identifier (with options for 'Remove any pre-existing tag', 'Use client tag', and 'Apply this VLAN tag'), Encryption (set to 'Disabled'), Encryption Protocols (with checkboxes for IPSEC, L2TP+IPSEC, PPTP, and SSH), MPPE (set to 'Stateless'), Key Length (set to '128 bits'), Authentication Method (with options for 'Use Associated Authentication Policy' and 'Use shared secret'), and MSCHAP (set to 'V2 only'). At the bottom of the form are 'Save' and 'Cancel' buttons.

To create or edit an Access Policy,

- Step 1.** Type a name for the policy in the **Name** field. You can change the name of an existing Access Policy by typing a new name.
- Step 2.** Select settings or enter data on each of the tabs as appropriate. See the sections below for a detailed discussion of each tab.
- Step 3.** Click **Save** to save this Access Policy. If you are editing an existing Access Policy, this replaces the original Access Policy with the modified Access Policy definition.

To add the modified Access Policy as a new Access Policy, leaving the original Access Policy unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Access Policy page.

After a **Save As Copy** the page remains displayed so you can make additional changes.

Click **Cancel** to return to the previous page without making any further changes.

Note: To have your changes affect currently connected clients, you must go to the Client Status page and refresh user rights. Otherwise, any changes you make take effect the next time a client gets new rights. Changes **do not** automatically affect connected clients.

The Settings Tab

On the **Settings** tab, select or enter data into the fields as described in Table 4-16 below.

The fields under the **Settings** tab are as follows:

Table 4-16. New Access Policy Settings Tab Contents

Column	Description
Network Address Translation	<p>Whether Network Address Translation (NAT) should be used for a client under this Access Policy.</p> <ul style="list-style-type: none"> Select Always (the default) to have the 700wl Series system use NAT addresses for clients in all circumstances. Do not use this if clients authenticate using NT Domain logon Select When Necessary to have the 700wl Series system 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). This is the recommended setting when you want clients to use a real (DHCP-provided) or static IP address. An external DHCP server must be available to provide these DHCP addresses. The Never setting forces the 700wl Series system to use the actual IP address presented by the client, regardless of whether it appears to be a valid address or not. If the IP address is not valid, all traffic from that client is dropped. <p>The Never setting should <i>not</i> be used for Access Policies that will apply to normal user clients. It should be used only in special cases, such as where a client device must respond to proxy ARP from the network (upstream).</p>
IP Addressing	<p>Whether clients may use static IP addresses, or whether addresses must be provided by DHCP. This setting is ignored if the NAT setting is Always.</p> <ul style="list-style-type: none"> Select Require DHCP if static IP addresses are not accepted. Select Allow Static IP to allow static IP addresses.

Table 4-16. New Access Policy Settings Tab Contents

Column	Description
VLAN Identifier	<p>How a VLAN Identifier (tag) should be handled:</p> <ul style="list-style-type: none"> • Select Remove any pre-existing tag to remove the VLAN tag (if any) associated with client packets, resulting in untagged traffic being forwarded onto the network. This is the default. • Select Use client tag to preserve the VLAN tag (if any) associated with client packets when forwarding traffic onto the network. • Select Apply this VLAN tag (and enter the tag) to tag all client traffic with the specified tag. Tag numbers can be between 1 and 4094. <p>See “VLANs and IP Addressing” on page 2-26 for a more extensive discussion of the use of VLANs within the 700wl Series system.</p>
Encryption	<p>Whether encryption is required, allowed, or disabled:</p> <ul style="list-style-type: none"> • Select Disabled to disable encryption for clients associated with this Access Policy. (This is the default.) • Select Allowed, but not required to allow both encrypted and non-encrypted traffic from clients associated with this Access Policy. The Encryption Protocols settings determine the type of encryption allowed. • Select Required to require all traffic from clients associated with this Access Policy to be encrypted. The Encryption Protocols settings determine the type of encryption required. Non-encrypted traffic is dropped. <p>Note: <i>If you require encryption, make sure that the protocols you select are enabled for the 700wl Series system on the Wireless Data Privacy page under the VPN functions area.</i></p> <p>See Chapter 7, “Setting up Wireless Data Privacy”, for a more extensive discussion of the use of VPNs within the 700wl Series system.</p>
Encryption Protocols	<p>The encryption protocols supported under this Access Policy, if encryption is allowed or required.</p> <ul style="list-style-type: none"> • Check one or more checkboxes to specify the protocols allowed or required. <p>Note: <i>Make sure that the protocols you select are enabled and configured appropriately.</i></p> <ul style="list-style-type: none"> • To view or change the IPSec encryption and secure hash algorithms or the enable/disable settings for the other protocols, click the Settings link that is part of the label for the IPSec checkbox, or click the VPN icon on the navigation toolbar. <p>Note: <i>The settings under the VPN icon are global—they apply to all uses of Wireless Data Privacy system-wide, not just to this Access Policy.</i></p>
MPPE (PPTP only)	<p>For PPTP, whether MPPE encryption should be stateful or stateless:</p> <ul style="list-style-type: none"> • Select Stateless to specify that the encryption key is reset for every packet. This is appropriate in a lossy environment, but is slower. This is the default. • Select Stateful to specify that the encryption key is reset once every 256 packets. This is appropriate in a low packet-loss environment, and is faster.

Table 4-16. New Access Policy Settings Tab Contents

Column	Description
Key Length (PPTP only)	<p>For PPTP, the minimum MPPE (RC4) session key length:</p> <ul style="list-style-type: none"> • Select 40 bits to allow a 40-bit or 128-bit key. This is the default. • Select 128 bits to allow a 128-bit key only. • Select no encryption to disable MPPE encryption.
Authentication Method	<p>For L2TP or PPTP, the method that should be used to authenticate users who connect and present a username and password via an L2TP or PPTP client:</p> <ul style="list-style-type: none"> • Select Use Associated Authentication Policy to use the Authentication Policy associated with the Connection Profile associated with this Access Policy. <ul style="list-style-type: none"> <i>Note: If this Access Policy is associated with different Connection Profiles through the Rights Assignment Table, then the Authentication Policy used for L2TP or PPTP may be different, depending on the Connection Profile the client matches. See “The Rights Assignment Table” on page 4-6 for more information on how Authentication Policies, Connection Profiles, and the Rights table interact.</i> <i>Note: For L2TP, there are restrictions on the Authentication Policy that may be used if PAP is not allowed. In this case, the Authentication Policy must include only RADIUS or the built-in authentication services. If PAP is allowed, any authentication service may be included.</i> • Select Use Shared Secret to set the secret a client presents to create a PPTP tunnel. Enter the secret twice in the fields provided. <ul style="list-style-type: none"> <i>Note: This shared secret is not used for client authentication. Once the connection is made, the client is presented with the web-based logon page, and is authenticated based on the appropriate Authentication Policy to determine what access is allowed to the network.</i>
MSCHAP	<p>For L2TP, whether MSCHAP V1 and/or PAP is allowed in addition to V2:</p> <ul style="list-style-type: none"> • Select V2 only to enable only MSCHAP V2. • Select V1 or V2 to enable both V1 and V2. • Check Allow PAP for L2TP to allow PAP for authentication. <p>Note: If the client is using the L2TP client provided by HP ProCurve, you must allow PAP.</p>

Network Address Translation and IP Addressing Considerations

The NAT settings in an Access Policy affect client IP addressing as follows:

- If NAT is required (the Access Policy NAT setting is **Always**) then the Access Controller *always* uses NAT mode. Static IP addresses are translated, and client DHCP requests are satisfied by the Access Controller’s internal DHCP server, and are then translated.
- If NAT is not required, but is allowed (the Access Policy NAT setting is **When Necessary**) then the client’s real or static IP address is used, untouched, unless the IP address is not valid. Client DHCP requests are satisfied by the external DHCP server, and the resulting address is used. A static IP addresses is used as is, unless it is determined to be 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 configured for it (through the Subnet tab under Interfaces in the Rights Manager) then an IP

Configuring Rights

address is valid if it falls within that address 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 falls within the Access Controller's subnet. NAT is used only if it is not within that subnet.

If the IP address is not valid, the Access Controller assigns a private IP address and rewrites the source address in packets.

Note: *With this setting it is possible that a client might receive a NAT'ed address initially, but when the client's DHCP lease expires, it might successfully get a valid real IP address, which would be used as the source IP instead of a NAT'ed address.*

- If NAT is *never* allowed (the Access Policy NAT setting is **Never**) the Access Controller or Integrated Access Manager always uses the client's real IP address (as obtained via DHCP) or its static IP address. If the address is valid on the port or Access Controller subnet, the address is left untouched as the source address in packets going to the network. If the client's IP address is not valid, however, traffic to and from the client is dropped.

Caution: *This setting is intended for use only in special cases. It should not be used for normal clients, including Access Points and other devices.*

Note: *It is recommended that you configure your IP address mode consistently across Access Policies that are related. For example, you should use the same NAT mode in the Access Policy you configure for unauthenticated clients and in the Access Policies that will affect those clients after they have authenticated.*

Using NAT has a number of benefits for the 700wl Series system, especially in relation to roaming. If a client has a NAT'ed IP address, when it roams to a different Access Controller its sessions can actually be moved to the new Access Controller rather than being tunneled back through the original Access Controller. If the client is using a real IP address, all sessions must be tunneled back through the original Access Controller.

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 NAT setting in the Access Policy.

Note: *A side-effect of this behavior is that if encryption is "Allowed but not Required" in the Access Policy, and a client connects without using a tunneling protocol, that client will always receive a NAT'ed IP address upon making a DHCP request. The client will avoid being NAT'ed 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 Access Policy NAT setting, 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.

The Allowed Traffic Tab

Allowed Traffic filters are traffic filters that identify packets that are permitted to be forwarded by an Access Controller.

If you are creating a new Access Policy, the Allowed Traffic filters are displayed in alphabetical order. If you are editing an Access Policy, the traffic filters that are included in this Access Policy are displayed at the top of the list, and the remaining filters that are not included in this Access Policy are at the bottom of the list.

To select Allowed Traffic filters to include in this Access Policy, select the **Allowed Traffic** tab, as shown in Figure 4-25, then select the Allowed Traffic Filters you want to include.

Configuring Rights

Figure 4-25. Creating an Access Policy, the Allowed Filters Tab

The screenshot displays the HP ProCurve management interface. At the top, the HP logo and 'invent' tagline are visible on the left, and user information (Username: admin, Access Control Server: 192.168.10.116, Date & Time: Mon Mar 1 12:41:04 2004) is on the right. A navigation bar includes icons for STATUS, RIGHTS, NETWORK, VPN, MAINT, LOGS, HELP, and a LOGOUT button. Below this, a menu bar highlights 'Access Policies' among other options like Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Logon Customization, and Tools & Options.

The main content area is titled 'New Access Policy'. It features a 'Name' input field and a series of tabs: Settings, Allowed Traffic (selected), Redirected Traffic, HTTP Proxy, Bandwidth, and Timeout. To the left of the 'Allowed Traffic' tab, there is instructional text: 'Provide a name for the Access Policy and specify its properties under the tabbed headings as follows:' followed by a list of bullet points detailing the configuration steps for each tab. Below this text, it says 'When finished, click Save.'

The 'Allowed Traffic' tab contains a table of filters. The table has two columns: 'Filter' and 'Details'. Each row represents a filter type with a checkbox in the 'Filter' column and a pencil icon in the 'Details' column. The filters listed are:

Filter	Details
<input type="checkbox"/> AC HTTPS Logon page	
<input type="checkbox"/> AC Logon-fwd append URI	
<input type="checkbox"/> AC Logon-fwd no URI	
<input type="checkbox"/> AC SSL Stop page	
<input type="checkbox"/> AC Stop page	
<input type="checkbox"/> All IP traffic	
<input type="checkbox"/> Appletalk	
<input type="checkbox"/> CDP and WHMP	
<input type="checkbox"/> DHCP	
<input type="checkbox"/> DNS TCP 53	
<input type="checkbox"/> DNS UDP 53	
<input type="checkbox"/> External ACS UI	
<input type="checkbox"/> HTTP	
<input type="checkbox"/> Internal Adm in UI	
<input type="checkbox"/> Internal HTTP	
<input type="checkbox"/> Internal IAM UI	
<input type="checkbox"/> Internal rights UI	
<input type="checkbox"/> Kerberos	
<input type="checkbox"/> Outside World	
<input type="checkbox"/> Ping	
<input type="checkbox"/> SMB TCP 139	
<input type="checkbox"/> SMB UDP 137	
<input type="checkbox"/> SMB UDP 138	

At the bottom of the filter list, there is a 'New Filter...' button. Below the table, there are 'Save' and 'Cancel' buttons.

Note that if the filter you select is one of a DNS or WINS filter pair, you must also include the corresponding Redirected Traffic member of the pair in your Access Policy, to redirect traffic to the proper DNS or WINS server.

The Allowed Traffic list shows all existing Allowed Traffic filters. These are displayed in alphabetical order if you are creating a new Access Policy. If you are editing an Access Policy, the filters included in the policy are displayed at the top of the list. The following information is provided about each filter:

Table 4-17. Allowed Traffic List Definitions

Column	Description
Name	The name for the Allowed Traffic Filter.
Details	The optional description of the filter.

- » To select a filter to include in this Access Policy, click the appropriate checkbox.
- » To create a new filter, click the **New Filter...** button at the bottom of the table.
- » To edit a filter, click the filter name or the pencil icon at the end of the row. This takes you directly to the Edit Filters page.

The 700wl Series system provides a number of predefined Allowed Traffic filters, as listed in Table 4-18.

Table 4-18. Predefined Allowed Traffic Filters

Allowed Traffic Filter	Description
All IP Traffic	Allows all IP packets to be forwarded
AC HTTPS Logon page	Allows access to Access Controller SSL logon page via 42.0.0.1
AC Logon-fwd append URI	Allows requests to port 82 (Access Controller logon page), which preserves the original destination URL
AC Logon-forward no URI	Allows requests to port 83 (Access Controller logon page), which does not preserve the original destination URL
AC SSL Stop page	Allows requests to the Access Controller SSL Stop page
AC Stop page	Allows requests to the Access Controller Stop page
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 client DHCP requests are properly handled
DNS TCP 53*	Allows DNS requests via TCP port 53
DNS UDP 53*	Allows DNS requests via UDP port 53
External ACS UI	Allows access to the Access Control Server UI using the external IP address
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 IAM UI	Allows access to the Integrated Access Manager using the internal IP address (42.0.0.1)

Table 4-18. Predefined Allowed Traffic Filters

Allowed Traffic Filter	Description
Internal rights UI	Allows access to the Rights Manager pages via the Access Controller defined in @INTERNAL@ (by default 42.0.0.1)
IP Fragments	Allows subsequent packet fragments for packets that exceed the maximum packet size (1500 bytes)
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 UDP 137*	Allows the user to access to the netbios UDP port 137
SMB UDP 138*	Allows the user to access to the netbios UDP port 138
SMB TCP 139*	Allows the user to access to the netbios TCP port 139

* To allow DNS or SMB you must include both DNS filters or all three SMB filters in your Access Policy.

If these filters are not sufficient to meet your needs, you can create your own. See “Creating or Editing an Allowed Traffic Filter” on page 4-64 for instructions.

The Redirected Traffic Tab

Redirected Traffic filters are traffic filters that identify packets sent from a client that should be redirected to a new destination. Some Redirected Traffic filters 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. Redirected Traffic filters can also be used to prevent traffic from reaching a prohibited destination—in this case, the filter may redirect the request to the 700wl Series system Stop page, or other alternate destination as appropriate.

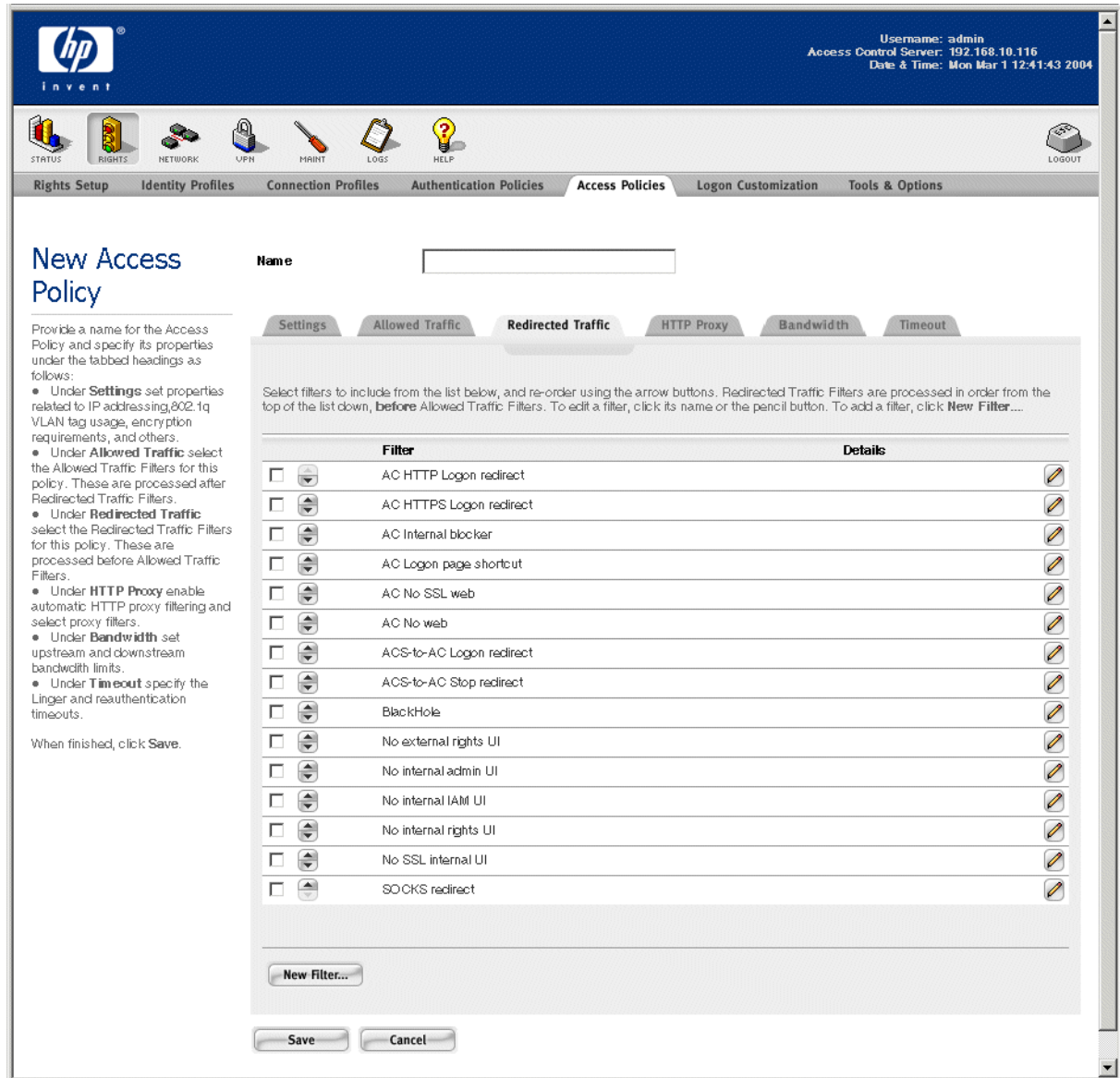
If you creating a new Access Policy, the Redirected Traffic Filters are initially displayed in alphabetical order.

If you are editing an Access Policy, the Redirected Traffic filters that have been selected for this Access Policy are displayed at the top of the list, in precedence order as specified for the filter. The filters that have not been selected for this Access Policy are at the bottom of the list.

To select Redirected Traffic filters to include in this Access Policy, select the **Redirected Traffic** tab, as shown in Figure 4-26. Then select the filters you want to include, reordering them if necessary to create the proper precedence relationships among the selected filters.

Note that if the filter you select is one of a DNS or WINS filter pair, you must also include the corresponding Allowed Traffic member of the pair in your Access Policy, to allow traffic to pass to the destination of the redirect.

Figure 4-26. Creating an Access Policy, the Redirected Traffic Tab



The Redirected Traffic list shows the following information about each filter:

Table 4-19. Redirected Traffic List Definitions

Column	Description
Name	The name for the Redirected Traffic Filter.
Details	The optional description of the filter.

- » To select a filter to include in this Access Policy, click the appropriate checkbox.
- » To move a filter up or down in the filter list, click the up or down button to the left of the filter name.

Configuring Rights

Note: *Redirected Traffic filters are evaluated in the order that they appear in the Redirected traffic list of each Access Policy. When a packet matches a Redirect filter, it is immediately redirected to the appropriate destination. Therefore, an incorrect ordering of Redirect filters could cause some filters never to be evaluated. For example, if a more general filter is evaluated before a more specific filter, packets could be redirected due to matching the general filter, and never be evaluated by the more specific filter.*

Reordering the filter list affects only the Access Policy that is currently being created. Each Access Policy may use a different ordering of Redirect filters.

- » To create a new filter, click the **New Filter...** button at the bottom of the table.
- » To edit a filter, click the filter name or the pencil icon at the end of the row. This takes you directly to the Edit Filters page. Note that if the filter is one of a DNS or WINS filter pair, this takes you to the Edit Filters page for the pair.

The 700wl Series system provides a number of predefined Redirected Traffic filters, as listed in Table 4-20.

Table 4-20. Predefined Redirected Traffic Filters

Redirected Traffic Filter	Description
AC 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.
AC HTTPS Logon redirect	Redirects most HTTPS requests on port 443, the standard SSL port, to the Access Controller SSL logon page on port 443.
AC Internal blocker	Redirects HTTP requests intended for addresses within the Access Control Server subnet (@INTRANET@) to the Access Controller Stop page.
AC Logon page shortcut	Redirects HTTP requests intended for 1.1.1.1 port 80 to the Access Controller logon page.
AC No SSL Web	Redirects all HTTPS requests on port 443, the standard SSL port, to the Access Controller SSL Stop page.
AC No Web	Redirects all HTTP requests on port 80 to the Access Controller Stop page.
BlackHole	Redirects all requests except for DHCP, DNS, Stop page and HTTP requests to 0.0.0.0. This effectively prevents network access.
ACS-to-AC 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.
ACS-to-AC 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.
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

Table 4-20. Predefined Redirected Traffic Filters

Redirected Traffic Filter	Description
No internal IAM UI	Redirects Integrated Access Manager UI access requests via 42.0.0.1
No internal rights UI	Redirects Rights Manager UI access requests via 42.0.0.1 to the SSL Stop page
No SSL internal UI	Redirects SSL Administrative Interface access requests via 42.0.0.1 to the SSL Stop page
SOCKS redirect	Redirects all SOCKS requests to the Access Controller

If these filters are not sufficient to meet your needs, you can create your own filters. See “Creating or Editing a Redirected Traffic Filter” on page 4-67 for instructions.

The HTTP Proxy Tab

The Automatic HTTP Proxy feature of the 700w1 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. The configuration of an HTTP Proxy Server is done globally for the 700w1 Series system, in the Network Setup module.

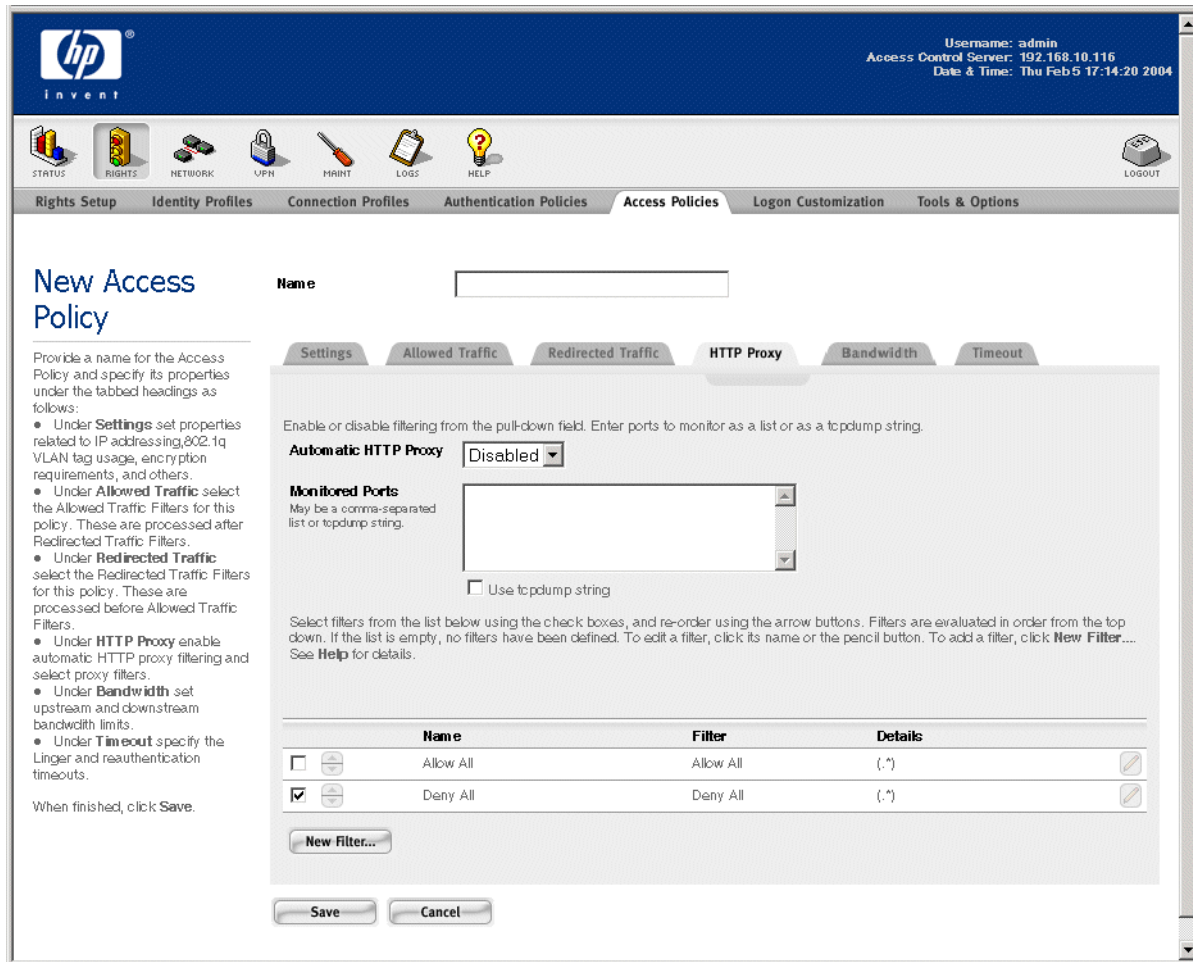
Within an Access Policy you can specify a set of proxy filters that will allow or deny HTTP traffic based on the destination of that traffic. You can specify which ports should be monitored for HTTP traffic to filter, and you can create filter rules based on fully-qualified domain names, IP addresses, simple host names, network addresses (subnets), or any arbitrary destination based on matching a regular expression. HTTP requests that are denied based on these filter rules are redirected to the Stop page.

Note: *If you do not configure a proxy server, but you configure and enable the automatic proxy feature within an Access Policy, the 700w1 Series system will act as the proxy server, and will handle the traffic according to the configured ports and filters. See “Automatic HTTP Proxy Server Specification” on page 6-26 in Chapter 6 for instructions on configuring the IP address of your Proxy server.*

Configuring Rights

To configure automatic HTTP Proxy filtering for this Access Policy, select the **HTTP Proxy** tab, as shown in Figure 4-27, and select or enter data into the fields as described in Table 4-21.

Figure 4-27. Creating an Access Policy, the HTTP Proxy Tab



The fields under the **HTTP Proxy** tab are as follows:

Table 4-21. HTTP Proxy Tab Field Definitions

Field/Column	Description
Automatic HTTP Proxy	Enables or disables automatic HTTP proxy filtering for this Access Policy. <ul style="list-style-type: none"> Select the appropriate setting (Enabled or Disabled) from the drop-down list. The default is Disabled.
Monitored Ports	A list of ports or port ranges that should be monitored for HTTP traffic to filter. <ul style="list-style-type: none"> To enter a colon-separated list of ports or port ranges, type the list into the field provided. You can also enter the list using commas as separators.
Filter	The filter type. The choices are: <ul style="list-style-type: none"> Allow IP Accept HTTP traffic destined for the specified IP address

Table 4-21. HTTP Proxy Tab Field Definitions

Field/Column	Description
• Allow FQDN	Accept HTTP traffic destined for the specified fully-qualified domain name (e.g. <code>www.domain.com</code>)
• Allow Host	Accept HTTP traffic destined for the specified host name (e.g. <code>www</code> or <code>home</code>)
• Allow Net	Accept HTTP traffic destined for the specified network address (IP address and subnet mask) (e.g. <code>192.168.0.0/16</code>)
• Allow Reg	Accept HTTP traffic with destination specified as a regular expression that evaluates to an address or address range (for example <code>(.*)domain.com</code>)
• Deny IP	Redirect HTTP traffic destined for the specified IP address
• Deny FQDN	Redirect HTTP traffic destined for the specified fully-qualified domain name (e.g. <code>www.domain.com</code>)
• Deny Host	Redirect HTTP traffic destined for the specified host name (e.g. <code>www</code> or <code>home</code>)
• Deny Net	Redirect HTTP traffic destined for the specified network address (IP address and subnet mask) (e.g. <code>192.168.0.0/16</code>)
• Deny Reg	Redirect HTTP traffic with destination specified as a regular expression that evaluates to an address or address range (for example <code>(.*)domain.com</code>)
• Allow All	Accept all other HTTP traffic. The destination is always specified as <code>(.*)</code> . This is the alternate catch all rule
• Deny All	Redirect all other HTTP traffic. The destination is always specified as <code>(.*)</code> . This is the default catch all rule
An Accept rule forwards the traffic to the proxy server; a Deny rule drops the packet and redirects the client to the Stop page.	
Details	The specification of the destination, as appropriate for the type of filter.

- To select a filter to include in this Access Policy, click the appropriate checkbox.
- To move a filter up or down in the filter list, click the up or down button to the left of the filter name.

Note: HTTP Proxy filters are evaluated in the order that they appear in the HTTP Proxy filters list of each Access Policy. When a packet matches a HTTP Proxy filter, it is immediately redirected to the appropriate destination. Therefore, an incorrect ordering of HTTP Proxy filters could cause some filters never to be evaluated. For example, if a more general filter is evaluated before a more specific filter, packets could be redirected due to matching the general filter, and never be evaluated by the more specific filter.

Reordering the filter list affects only the Access Policy that is currently being created. Each Access Policy may use a different ordering of HTTP Proxy filters.

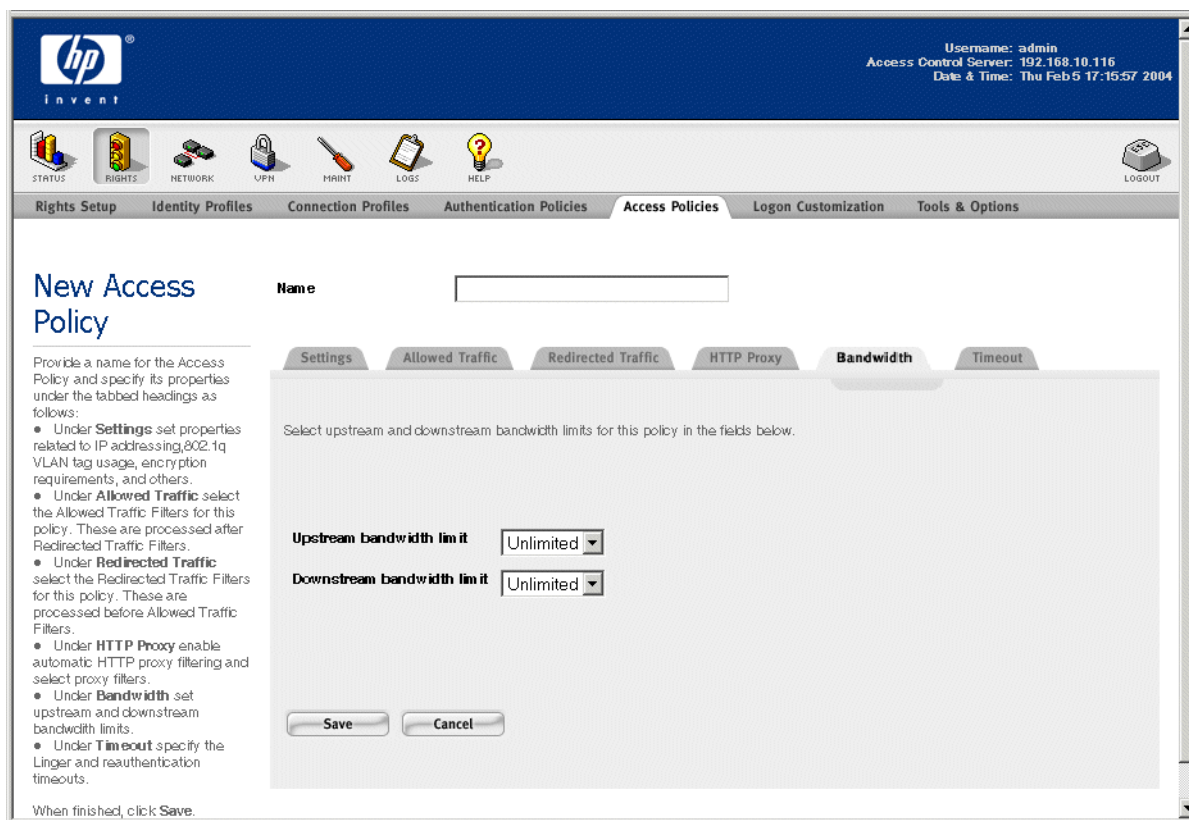
- To edit a filter, click the filter name or the pencil icon at the end of the row. this takes you directly to the Edit Filters page.

The Bandwidth Tab

700wl Series system version 4.0 provides the ability to limit the bandwidth available to each client to prevent network performance degradation. Using Access Policies, bandwidth can be limited on a client by client basis. Separate limits can be set for upstream and downstream bandwidth.

On the **Bandwidth** tab, as shown in Figure 4-28, select or enter data into the fields as described in Table 4-22 below.

Figure 4-28. Creating an Access Policy, the Bandwidth Tab



The fields under the **Bandwidth** tab are as follows:

Table 4-22. Bandwidth Tab Field Definitions

Column	Description
Upstream bandwidth limit	Bandwidth limit for traffic from a client: <ul style="list-style-type: none"> • Select a bandwidth setting from the drop-down list. The default is Unlimited.
Downstream bandwidth limits	Bandwidth limit for traffic to a client: <ul style="list-style-type: none"> • Select a bandwidth setting from the drop-down list. The default is Unlimited.

Bandwidth Rate Limiting in the 700wl Series system

700wl Series system version 4.0 provides bandwidth rate limiting (or “policing”) on a per-client basis. Each client may use bandwidth as necessary up to the upstream or downstream limit set by the Access Policy currently in force for that client. This implementation does not attempt to shape bandwidth usage, just enforces a per-client cap.

Because bandwidth limits are set in the Access Policy, you can set different limits for different sets of clients even if they are connecting through the same physical port. The bandwidth limit is imposed per client—even if there is additional bandwidth available on the specific port, a given client will be limited to the specified limit, and cannot take advantage of the additional unused bandwidth.

For non-TCP traffic, these bandwidth limits work in a straightforward manner. For TCP traffic, there are some performance considerations that may limit the throughput to less than the configured limit, especially if client traffic is being encrypted (using IPSec or PPTP).

If a client is logged onto the 700wl Series system using PPTP or IPSec for encryption, a certain amount of overhead related to packet encryption may somewhat reduce the actual throughput experienced relative to the specified throughput. If encrypted traffic is tunneled between Access Controllers due to client roaming, throughput may be further affected. When a client roams between Access Controllers, existing client sessions are tunneled through the new Access Controller back to the original Access Controller. For non-encrypted traffic, new sessions initiated after the roam may be handled directly by the new Access Controller, but even new sessions involving encrypted traffic are tunneled back to the original Access Controller. For non-encrypted traffic that is tunneled, bandwidth limits are enforced both on the new Access Controller (to avoid tunneling packets that should be dropped) and on the original Access Controller, which makes the actual determination of whether to drop packets. However, with encrypted packets the new Access Controller cannot determine which packets should be dropped and thus tunnels all to the original Access Controller.

If the 700wl Series system is used to pass through encrypted traffic and is not the termination of the VPN, the bandwidth limitation algorithm cannot use the packet contents to help determine which packets to drop. In this case, it adopts a very conservative algorithm to ensure that throughput will not exceed the configured limits, and in this case may in fact result in throughput below the configured limits.

In general, when setting bandwidth limits, you may need to adjust your bandwidth settings based on actual client experience. If clients are experiencing bandwidth significantly below the configured limits, you may want to increase the limits so that throughput more closely approaches the limits you intend.

Note: *If you are measuring throughput at layer 2, the actual bandwidth includes headers, acknowledgements etc. in addition to the data itself, and these must be taken into account—such as transferring a 10 megabit file via FTP at 1Mbit/sec. will take more than 10 seconds due to the additional information involved in the transfer.*

The Timeout Tab

On the Timeout tab, you can specify two types of timeouts:

- The *Linger Timeout*, which specifies how long the 700wl Series system will continue to consider a client active after the Access Controller has determined that the client is no longer connected and has disassociated the client.
- A reauthentication timeout, which specifies a time limit on the validity of a user’s authentication, even if the user has been continuously connected and active.

The Linger Timeout

The Linger timeout enables the 700wl Series system to force a logoff for clients that have disconnected from the network without logging off. If the Access Controller determines that a client has been non-responsive for a specified period of time, the Access Controller sends a disassociate message to the Access Control Server, following which the Linger Timeout starts. If the Linger Timeout expires and the client has not reappeared, the Access Control Server logs that client off the system. This prevents clients that are no longer connected from consuming system resources as if they were still active.

When a client roams from one Access Point to another, there is typically a time lag between when it disappears from its original port (and thus appears idle and non-responsive to the Access Controller) and when it reappears, possibly on a different port and/or Access Controller. The Linger Timeout provides an interval during which the client can complete a roam without having its open sessions terminated.

The Access Controller idle timer and polling timeout (which determines how long it takes the Access Controller to decide that the client is no longer connected) are set under the Advanced Setup tab of the Network Setup page. See “Access Controller Advanced Configuration Options” on page 6-24 for more information.

The Reauthentication Timeout

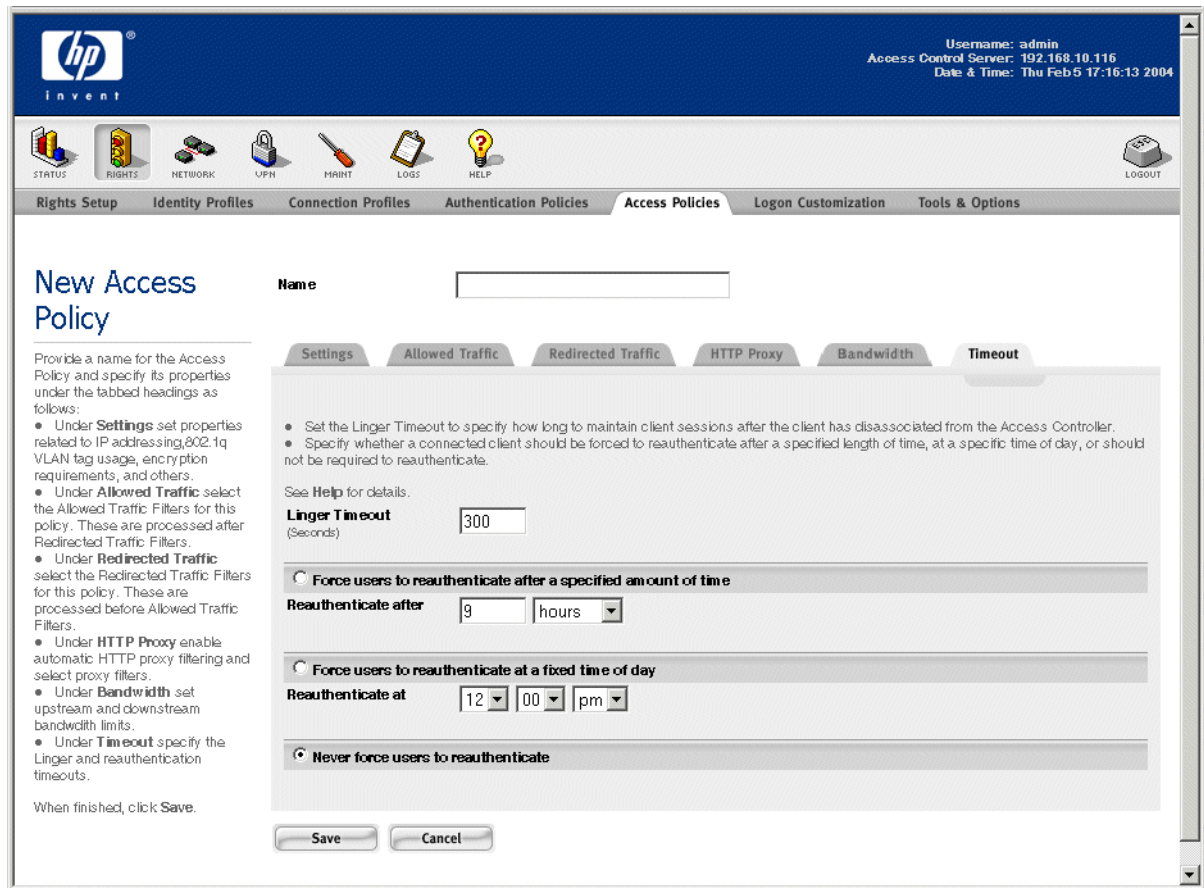
The remaining fields on the Timeout tab let you specify how long a client’s rights remain valid before they are required to reauthenticate. If you set a reauthentication timeout, users will be required to reauthenticate (log in again) periodically, even if they have remained connected and active the entire time.

For example, if you check **Force users to reauthenticate after a specified amount of time**, and set the interval to two hours, then any client getting rights through this Access Policy will have to reauthenticate every two hours.

You can specify reauthentication as an interval (some number of minutes, hours, or days) or as a fixed time of day. The default is to not require reauthentication at all.

On the **Timeout** tab, as shown in Figure 4-29, select or enter data into the fields as described in Table 4-23 below.

Figure 4-29. Creating an Access Policy, the Timeout Tab



The fields under the **Timeout** tab are as follows:

Table 4-23. Timeout Tab Field Definitions

Field	Description
Linger Timeout	<p>How long a client remains known to the 700wl Series system after being disassociated from an Access Controller for failing to respond to repeated polls (ARPs).</p> <ul style="list-style-type: none"> Enter the number of seconds the system should wait before logging off the client from the system. <p>This timeout functions in concert with the client polling settings specified in the Network module. See “Client Polling” on page 6-25 for more information.</p>
Force users to reauthenticate after a specified amount of time	<p>Forces reauthentication after a client has been connected for a specified period of time:</p> <ul style="list-style-type: none"> Check the radio button, then select a time period (number and time unit) from the drop down lists.
Force users to reauthenticate at a fixed time of day	<p>Forces reauthentication of all clients at a fixed time of day:</p> <ul style="list-style-type: none"> Check the radio button, then select a time of day from the drop-down lists.

Table 4-23. Timeout Tab Field Definitions

Field	Description
Never force users to reauthenticate	Allows client sessions to remain connected indefinitely without requiring reauthentication. • Check the radio button to select this option. This is the default.

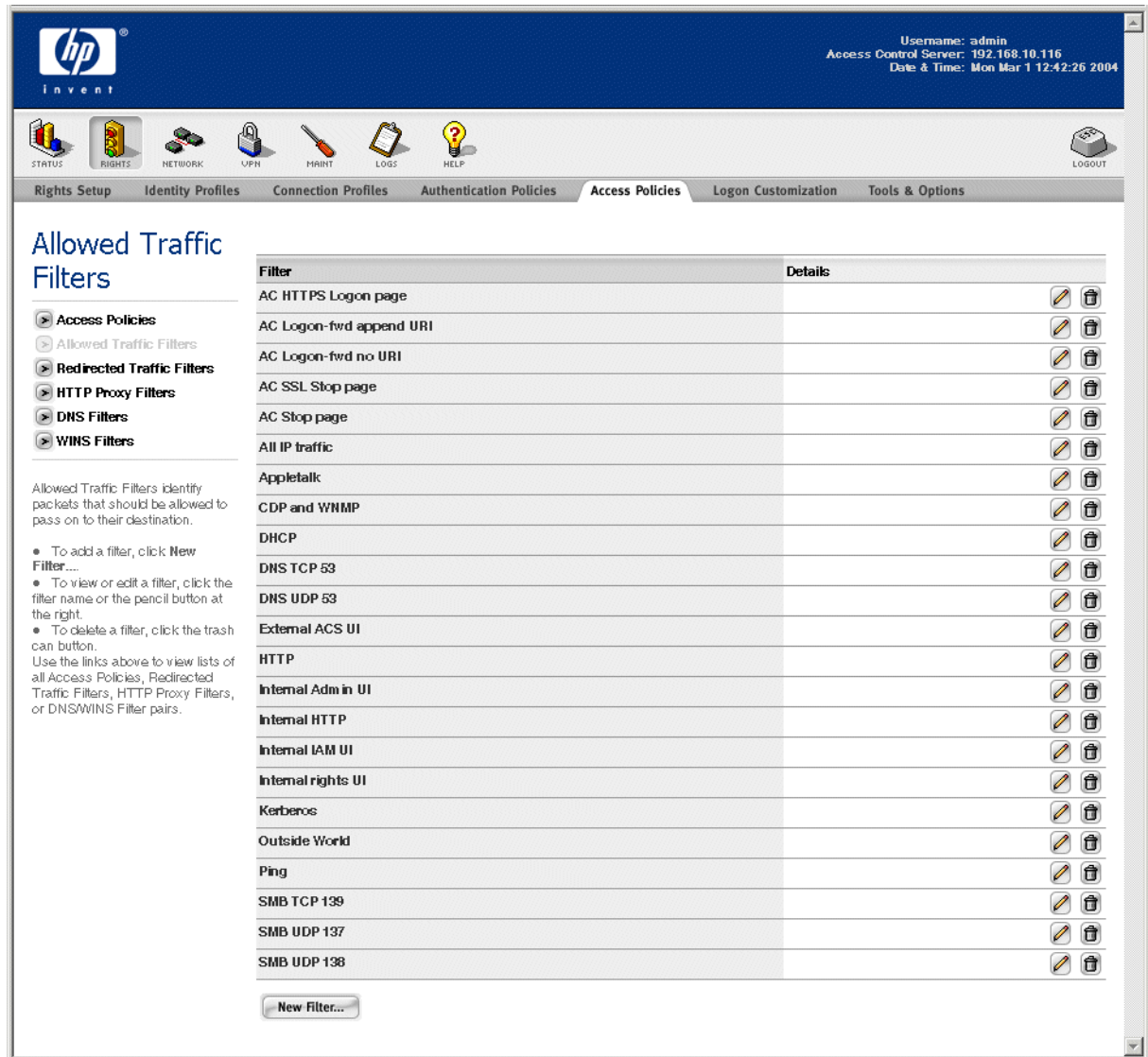
Allowed Traffic Filters

Allowed Traffic filters are traffic filters that identify packets that are permitted to be forwarded by an Access Controller. The 700wl Series system provides a number of predefined Allowed Traffic filters that you can select to include in an Access Policy. Table 4-18 on page 4-51 lists the predefined Allowed Traffic filters provided by the 700wl Series system.

If the predefined filters are not sufficient for your needs, you can define additional filters, or modify the existing filters.

- » To view the list of Allowed Traffic Filters currently defined in the 700wl Series system, click the **Allowed Traffic Filters** link on the main Access Policies page. The Allowed Traffic Filters page appears, as shown in Figure 4-30.

Figure 4-30. The Allowed Traffic Filters List



The Allowed Traffic list shows the Allowed Traffic filters in alphabetical order, and includes the following information about each filter:

Table 4-24. Allowed Traffic List Definitions

Column	Description
Name	The name for the Allowed Traffic Filter.
Details	The optional description of the filter.

- » To edit a filter, click the filter name in the Name column, or click the pencil icon at the end of the row. This takes you directly to the Edit Filter: Allowed Traffic page to edit the entry for this user (see “Creating or Editing an Allowed Traffic Filter” on page 4-64).

Configuring Rights

- » To delete a filter, click the trash can icon at the end of the row.
- » To create a new filter, click the **New Filter...** button at the bottom of the filter list. This takes you to the New Filter: Allowed Traffic page (see “Creating or Editing an Allowed Traffic Filter”).

From this page you can also go directly to the Access Policies, Redirected Traffic Filters, or HTTP Proxy Filters pages using the links directly under the page name in the left-hand panel of the page. See “Access Policies” on page 4-39, and “Time Windows” on page 4-37 for details on these functions.

Creating or Editing an Allowed Traffic Filter

To create a new Allowed Traffic Filter, click the **New Filter...** button found either on the Allowed Traffic Filters page or under the Allowed Traffic tab on the New Access Policy or Edit Access Policy pages.

The New Filter: Allowed Traffic page appears (Figure 4-31) with blank fields.

The Edit Filter: Allowed Traffic page is almost identical to the New Filter page, except that the name, description, and settings are displayed for the filter you have selected, and a **Save As Copy** button is provided.

Figure 4-31. Creating a New Allowed Traffic Filter

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes tabs for Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies, Logon Customization, and Tools & Options. The main content area is titled "New Filter: Allowed Traffic" and contains the following instructions:

- Enter a name and description for the filter.
- Specify the traffic filter by protocol, port, and address, or by providing a custom filter definition in tcpdump syntax. Use an asterisk (*) to indicate all ports, or any IP address. The address can also be a user-defined or built-in address variable.
- Click a View button to see built-in port definitions and built-in or user-defined address variable definitions.
- See Help for details.

When finished, click Save.

The configuration form includes the following fields and options:

- Name:** Text input field.
- Description:** Text input field.
- Allow traffic based on specific protocol/port/address:** Radio button (selected).
 - Protocol:** Dropdown menu (IP).
 - Port:** Text input field with a View button.
 - Address:** Text input field with a View button.
- Allow traffic via a custom filter:** Radio button (unselected).
 - Filter:** Text input field (in tcpdump syntax).


At the bottom of the form are **Save** and **Cancel** buttons.

You can create the filter specification in one of two ways:

- Specify the traffic protocol, and the destination IP address and port, or
- Define the filter as a regular expression in tcpdump syntax. This enables you to define complex filters.


To create or edit an Allowed Traffic filter, do the following:

- Step 1.** Type a name for this filter. You can change the name of an existing Allowed Traffic filter by typing a new name.
- Step 2.** Type a description for the filter, or modify the existing description.
- Step 3.** To specify the filter by selecting the protocol, and providing the port and destination IP address, select the **Allow traffic via a specific protocol/port/address** radio button. Then do the following:
- Select the protocol of the traffic you want to allow from the drop-down list in the **Protocol** field.
 - 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.

You can access a list of ports by clicking the View icon () at the right of the **Port** field. This displays in a separate pop-up window a list of ports for common destinations such as the Stop pages or the Logon pages.

- 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” followed by a space to negate the address. For example: **not @INTERNAL@**.

You can access the list of built-in address variables by clicking the View icon () at the right of the **Address** field. This displays a separate window that lists both the built-in address variables and lets you create user-defined address variables. See Figure 4-34.

- Step 4.** To use a tcpdump expression to specify a filter, select the **Allow traffic via a custom filter** radio button, and type the appropriate expression into the text box. See [Appendix B, “Filter Expression Syntax”](#) for details of the tcpdump syntax.

You can create more complex filters using a tcpdump expression. 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)
```

Note: *Tcpdump syntax is case sensitive. All keywords must be in lower-case to be recognized.*

- Step 5.** Click **Save** to save this filter. If you have edited an existing filter, this replaces the original filter with the modified filter definition.

To add the modified filter as a new Allowed Traffic filter, leaving the original filter unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Filter page.

After a **Save As Copy** the same page remains displayed so you can make additional changes.

Click **Cancel** to return to the previous page without making any further changes.

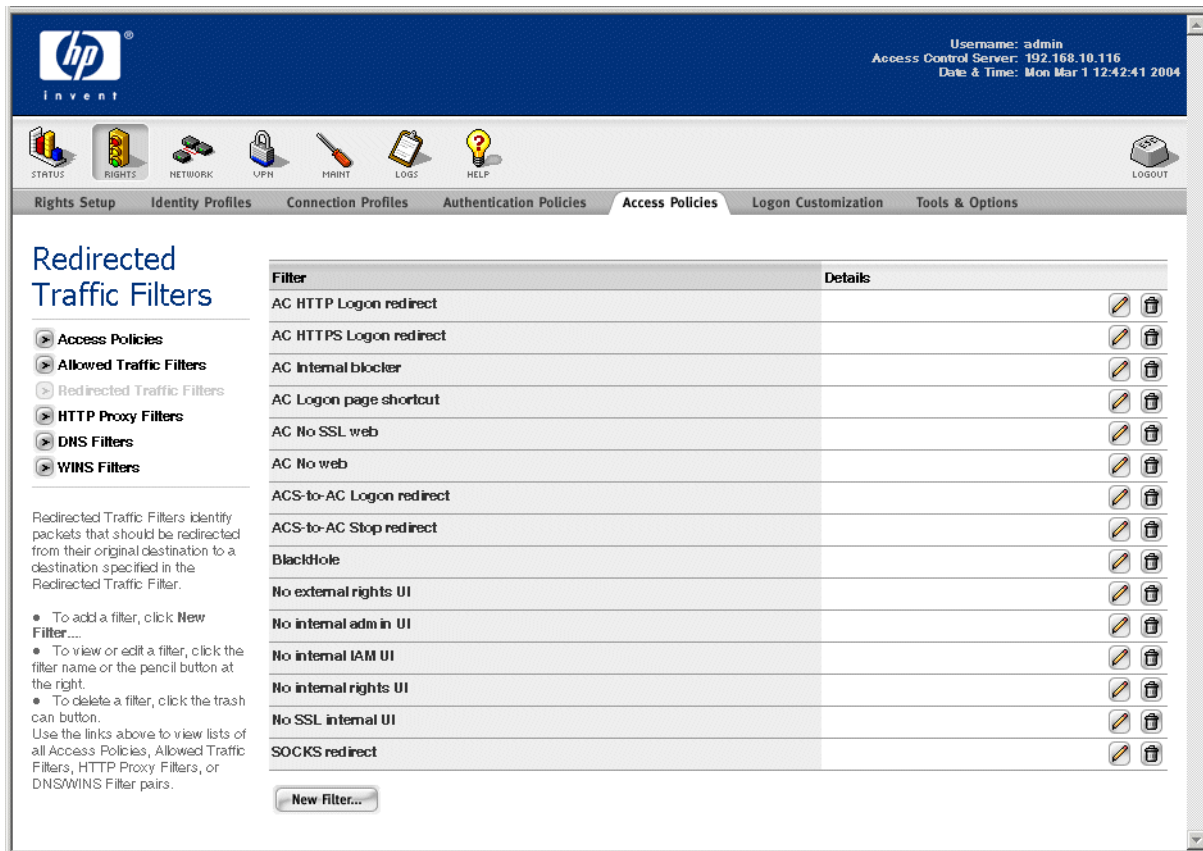
Redirected Traffic Filters

Redirected Traffic filters are traffic filters that identify packets sent from a client that should be redirected to a new destination. Some Redirected Traffic filters 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. Redirected Traffic filters can also be used to prevent traffic from reaching a prohibited destination—in this case, the filter may redirect the request to the 700wl Series system Stop page, or other alternate destination as appropriate.

The 700wl Series system provides a number of predefined Redirected Traffic filters that you can select to include in an Access Policy. Table 4-20 on page 4-54 lists the predefined Redirected Traffic filters provided by the 700wl Series system. If the predefined filters are not sufficient for your needs, you can define additional filters, or modify the existing filters.

- » To view the list of Redirected Traffic Filters currently defined in the 700wl Series system, click the **Redirected Traffic Filters** link on the main Access Policies page. The Redirected Traffic Filters page appears, as shown in Figure 4-32.

Figure 4-32. The Redirected Traffic Filters List



The Redirected Traffic list shows the Redirected Traffic filters in alphabetical order, and includes the following information about each filter:

Table 4-25. Allowed Traffic List Definitions

Column	Description
Name	The name for the Redirected Traffic Filter.
Details	The optional description of the filter.

- » To edit a filter, click the filter name in the Name column, or click the pencil icon at the end of the row. This takes you directly to the Edit Filter: Redirected Traffic page to edit the entry for this user (see “Creating or Editing a Redirected Traffic Filter” on page 4-67).
- » To delete a filter, click the trash can icon at the end of the row.
- » To create a new filter, click the **New Filter...** button at the bottom of the filter list. This takes you to the New Filter: Redirected Traffic page (see “Creating or Editing a Redirected Traffic Filter”).

From this page you can also go directly to the Access Policies, Redirected Traffic Filters, or HTTP Proxy Filters pages using the links directly under the page name in the left-hand panel of the page. See “Access Policies” on page 4-39, and “Time Windows” on page 4-37 for details on these functions.

Creating or Editing a Redirected Traffic Filter

To create a new Redirected Traffic Filter, click the **New Filter...** button found either on the Redirected Traffic Filters page or under the Redirected Traffic tab on the New Access Policy or Edit Access Policy pages.

The New Filter: Redirected Traffic page appears (Figure 4-33) with empty fields.

The Edit Filter: Redirected Traffic page is almost identical to the New Filter page, except that the name, description, and the filter and destination definitions are displayed for the filter you have selected, and a **Save As Copy** button is provided.

Figure 4-33. Creating a New Redirected Traffic Filter

hp
invent

Username: admin
Access Control Server: 192.168.10.116
Date & Time: Mon Mar 1 13:06:48 2004

STATUS RIGHTS NETWORK VPN MAINT LOGS HELP LOGOUT

Rights Setup Identity Profiles Connection Profiles Authentication Policies **Access Policies** Logon Customization Tools & Options

New Filter: Redirected Traffic

- Enter a name and description for the filter.
- Specify the traffic filter by protocol, port, and address, or by providing a custom filter definition in tcpdump syntax.
- Specify the destination port and address to which the filtered traffic should be redirected.

Use an asterisk (*) to indicate all ports or any IP address. An address can also be a user-defined or built-in address variable.

Click a View button to see built-in port definitions and built-in or user-defined address variable definitions.

See [Help](#) for details.

When finished, click Save.

Redirect traffic based on a specific protocol/port/address

Protocol: IP
Port:
Address:

Redirect traffic via a custom filter

Filter (in tcpdump syntax):

Redirect traffic to the following port/address

Port:
Address:

Save Cancel

You can create the filter specification in one of two ways:


- Specify the traffic protocol, and the destination IP address and port, or
- Define the filter as a regular expression in tcpdump syntax. This enables you to define complex filters.

You specify the new destination by providing a port and IP address that the traffic should be redirected to.

To create or edit a Redirected Traffic filter, do the following:


- Step 1.** Type a name for this filter. You can change the name of an existing Allowed Traffic filter by typing a new name.
- Step 2.** Type a description for the filter, or modify the existing description.
- Step 3.** To specify the filter by selecting the protocol, and providing the port and destination IP address, select the **Capture traffic via a specific protocol/port/address** radio button. Then do the following:
 - 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.

You can access a list of ports by clicking the View button () at the right of the **Port** field. This displays in a separate pop-up window a list of ports for common destinations such as the Stop pages or the Logon pages.

- 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” followed by a space to negate the address. For example: **not @INTERNAL@**.

You can access the list of built-in address variables by clicking the View button () at the right of the **Address** field.


- Step 4.** To use a tcpdump expression to specify a filter, select the **Capture traffic via a custom filter** radio button, and type the appropriate expression into the text box. See [Appendix B, “Filter Expression Syntax”](#) for details of the tcpdump syntax.

You can create more complex filters using a tcpdump expression. 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)
```

Note: *Tcpdump syntax is case sensitive. All keywords must be in lower-case to be recognized.*

- Step 5.** In the **Redirect To** section, type the port and IP Address that the packet should be redirected to.

You can access a list of ports by clicking the View button () at the right of the **Port** field. This displays in a separate pop-up window a list of ports for common destinations such as the Stop pages or the Logon pages.

You can access the list of built-in address variables by clicking the View button at the right of the **Address** field. See “Built-in and User-defined Address Variables” on page 4-70 for details of this window.

For example, to redirect packets to the Stop page, you would specify port 81 at address @INTERNAL@ (the Access Control Server).

Note: *You must also have the ACS-AC Stop redirect enabled in the Access Policy for a redirect to the Stop page to work.*

- Step 6.** Click **Save** to save this filter. If you have edited an existing filter, this replaces the original filter with the modified filter definition.

To add the modified filter as a new Redirected Traffic filter, leaving the original filter unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Filter page.

After a **Save As Copy** the same page remains displayed so you can make additional changes.

Configuring Rights

Click **Cancel** to return to the previous page without making any further changes.

Built-in and User-defined Address Variables

For use in both Allowed and Redirected Traffic Filters, the 700w1 Series system provides a set of pre-defined address variables for various system components. These can be viewed (but not changed or deleted) in the Addresses tab of the pop-up window. User defined variables can be added, edited and deleted.


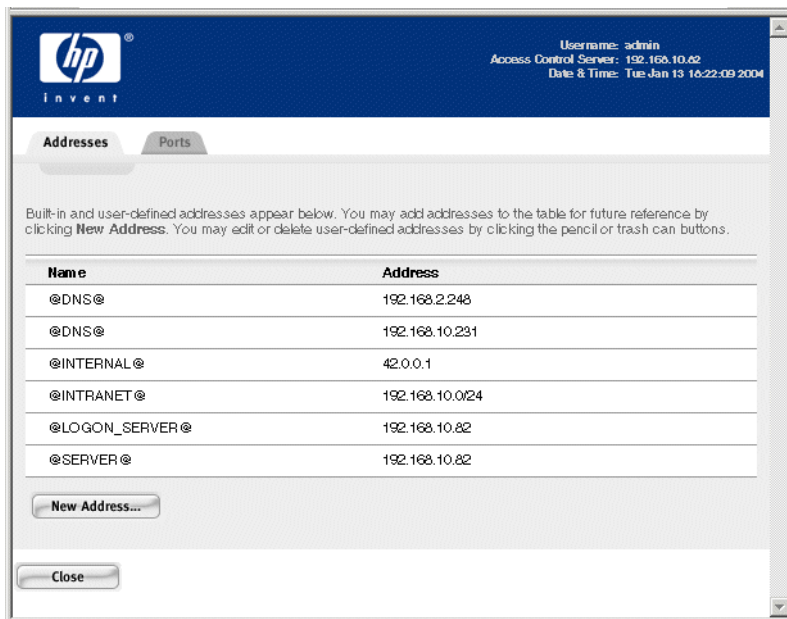
The Ports/Addresses pop-up window is accessed by clicking the **View** button () next to the **Ports** or **Addresses** field in the New Filters or Edit Filters pages for Allowed or Redirected Traffic filters. If you click the View button next to an Address field, the pop-up window appears with the Addresses tab displayed, as shown in Figure 4-34. If you click the View button next to the Ports field, the Ports tab is displayed when the window appears.

Figure 4-34. The Ports/Addresses pop-up window showing the Addresses tab



Address variables begin and end with an @. The Addresses list includes five predefined address variables. The @DNS@ address variable appears twice if both a primary and secondary DNS server are defined on the Network Setup page. The predefined variables are defined in Table 4-26.

Table 4-26. Predefined Address Variables

Address Variable	Value/Description
@DNS@	The two entries represent the primary and secondary DNS server addresses. When you use the @DNS@ variable in an Allowed Traffic filter (or in the filter portion of a Redirected traffic filter) the filter will match against either DNS address When you use the @DNS@ variable as the destination of a traffic filter, then whenever the Redirect filter is applied, the 700w1 Series system randomly selects one of the two addresses as the destination.

Table 4-26. Predefined Address Variables

Address Variable	Value/Description
@INTERNAL@.	The address of the Access Control Server Administrative Console. By default this is 42.0.0.1, but if you have reconfigured the address range for the internal DHCP server used for providing NAT addresses, this will be the first address in that range.
@INTRANET@	The network address of the subnet on which the Access Control Server resides
@LOGON_SERVER@	The IP address of the Logon Access Control Server. In a redundancy/failover configuration, this is always the IP address of the original primary Access Control Server, and remains so even when failover has occurred and the original Access Control Server is no longer functioning. Logon requests to @LOGON_SERVER@ are redirected to the Access Control Server currently acting as primary
@SERVER@	The IP address of the Access Control Server. In a redundancy/failover configuration, this is the IP address of the Access Control Server currently acting as primary.

Four of the five built-in addresses can only be modified by changing the network configuration of your 700wl Series system through the Network Setup page. The exception is the @INTRANET@ address, which you can change by entering it as if it were a user variable.

You can modify the @INTRANET@ variable by creating a new @INTRANET@ variable and providing a different network address. This creates a new entry in the table and overrides the old value. You cannot replace any of the other pre-defined variables this way—they reflect the values input during the network setup, and can be changed only by changing the network configuration on the Network Setup tab under the Network button.

» To create a user-defined address variable, click **New Address...**

You can edit any user-defined variable by clicking on the variable name. User-defined variables will act as links to the Edit Address page.

The Edit Address page appears, as shown in Figure 4-35.

Figure 4-35. Creating or Editing an Address Variable

Table 4-27 defines these two fields:

Table 4-27. Edit Address fields

Field	Definition
Name	The name of the variable. May be up to 32 uppercase alphabetic characters (no numerals or other characters). You may include the "@" at the beginning and end, but do not need to—the system will add them if necessary.
Value	The value can be an IP address or host name, up to 255 characters in length. It can include the characters allowed for a fully-qualified host name—alphanumeric characters, period, dash, and slash.

You can modify the @INTRANET@ variable by creating a new @INTRANET@ variable and providing a different network address. The new definition replaces the old definition. You cannot replace any of the other pre-defined variables this way—they reflect the values input during the network setup, and can be changed only by changing the network configuration on the Network Setup tab under the Network button.

DNS/WINS Filter Pairs

The DNS or WINS servers specified as part of the Basic Setup of each 700w1 Series system component are used by the 700w1 Series system for doing address resolution for its own needs. In addition, by default, the primary DNS or WINS servers are used as the destination of the predefined DNS and WINS redirects. When a client sends an address resolution request, by default it is redirected to the primary DNS or WINS server.

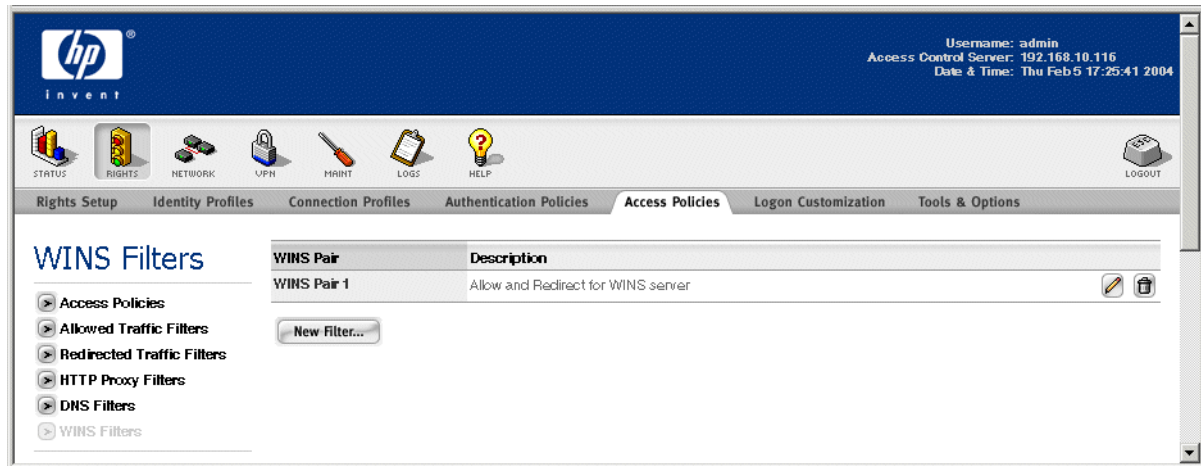
The DNS/WINS Filter feature lets you specify additional DNS or WINS servers, and create Allowed Traffic/Redirected Traffic filter pairs for those server destinations. The Redirected Traffic member of the pair redirects any DNS or WINS requests with unknown server destinations to (one of) the specified DNS or WINS servers. The Allowed Traffic member of the pair forwards a DNS or WINS request that has the specified server as the destination. You can specify multiple DNS or WINS servers, and then use those servers in the Allowed or Redirected Traffic filters. In a Redirect Traffic filter 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 a single server.

The Allowed and Redirected Traffic members of a DNS or WINS filter pair are created together in a single operation. Once created, they appear together with the other Allowed Traffic Filters or Redirected Traffic Filters under the Allowed Traffic/Redirected Traffic tabs available when you are creating or editing an Access Policy.

» To view the list of DNS filters currently defined in the 700w1 Series system, click the **DNS Filters** link on the main Access Policies page.

To view the list of WINS filters currently defined in the 700w1 Series system, click the **WINS Filters** link on the main Access Policies page. The WINS Filters page appears, as shown in Figure 4-36. The DNS Filters page looks identical.

Figure 4-36. WINS Filters List



The Filter list shows the DNS or WINS filter pairs in alphabetical order, and includes the following information about each pair:

Table 4-28. DNS or WINS Filter Pair list definitions

Column	Description
Name	The name of the filter pair.
Description	The optional description of the filter pair.

» To edit a filter pair, click the filter pair name in the Name column, or click the pencil icon at the end of the row. This takes you directly to the Edit Filter: DNS or Edit Filter: WINS page to edit the entry for this filter pair (see “Creating or Editing a DNS or WINS Filter Pair” on page 4-73).

You can also edit a filter pair by clicking the filter from either the Allowed Traffic tab or Redirected Traffic tab when you are creating or editing an Access Policy.

» To delete a filter pair, click the trash can icon at the end of the row.

» To create a new filter, click the **New Filter...** button at the bottom of the filter list. This takes you to the New Filter: DNS or New Filter: WINS page (see “Creating or Editing an HTTP Proxy Filter”).

From the DNS or WINS Filter list page you can also go directly to the Access Policies, Redirected Traffic Filters, Allowed Traffic Filters or HTTP Proxy Filters pages using the links directly under the page name in the left-hand panel of the page.

Creating or Editing a DNS or WINS Filter Pair

To create a new DNS filter pair or WINS filter pair, click the **New Filter...** button found on the DNS or WINS Filters pages.

The New Filter: WINS page or the New Filter DNS page appears with empty fields. Figure 4-37 shows the New Filter: DNS page. The New Filter: WINS page is almost identical.

Configuring Rights

The Edit Filter pages are almost identical to the New Filter pages, except that the name, description, and server definitions are displayed for the filter you have selected, and a **Save As Copy** button is provided.

Figure 4-37. Creating a New DNS Filter

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes tabs for Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies (selected), Logon Customization, and Tools & Options. The main content area is titled "New Filter: DNS". It contains a list of instructions for configuring the filter, a "Name" field with the value "DNS Filter Pair 1", and a "Description" field with the value "Allow and Redirect filters for alternate DNS". There are two radio button options for handling DNS servers: "Redirect other DNS Servers to one of the selected servers" (selected) and "Redirect other DNS Servers to the following server". The "DNS Servers" list contains "192.168.2.3" and "192.168.2.4". The "DNS Server" dropdown is set to "192.168.2.3". The "Modify DNS Server List" section has an "Add Server" button with "192.168.2.4" and a "Delete Server" button with "192.168.2.3". At the bottom are "Save" and "Cancel" buttons.

The first time you view one of these pages, the list of DNS or WINS servers will be empty. See Step 4 to manage the list of servers.

To create or edit a DNS or WINS filter pair, do the following:

Step 1. Type a name for this filter pair in the **Name** field. You can change the name of an existing HTTP Proxy filter by typing a new name.

Note: The name you provide here is used for both the Allowed Traffic and Redirected Traffic members of the filter pair.

Step 2. Type a description for the filter, or modify the existing description.

Step 3. In the middle region of the page, select how you want to handle the redirection of address resolution requests:

- To have the address resolution request redirected to one of multiple servers, select **Redirect other DNS servers to one of the selected servers** (or **Redirect other WINS servers to one of the selected servers** if you are creating or editing a WINS filter pair).

You must then select the servers you want from the server list. Select multiple servers from

the list, using the multi-select mechanism supported by your browser (typically Ctrl-click and Shift-click).

The 700w1 Series system selects a destination server at random from the servers you have selected, at the time rights are assigned to the client. That destination is used until the client reauthenticates and is given new rights, at which time a different destination server may be designated.

- To have the address resolution request redirected to a specific server, select **Redirect other DNS/WINS servers to the following server** and select a single server from the drop-down list.

Step 4. In the bottom region of the page, you can manage the list of DNS or WINS servers you want to use for address resolution requests. Initially, this list is empty. Once you have added servers to the list, they remain in the list.

- To add a server to the list, type the IP address of the server in the field provided, and click **Add Server**. The IP address should appear in the drop-down list immediately below the field where you entered the address, as well as in the two lists in the middle region of the page.
- To remove a server from the list, select the server from the drop-down list at the bottom of the page and click **Delete Server**. The selected server should disappear from the two lists in the middle region of the page as well as the list at the bottom of the page.

Step 5. Click **Save** to save this filter pair. If you have edited an existing filter, this replaces the original filter with the modified filter definition.

To add the modified filter pair as a new DNS or WINS filter pair, leaving the original filter pair unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Filter page.

After a **Save As Copy** the same page remains displayed so you can make additional changes.

Click **Cancel** to return to the previous page, abandoning any changes not yet saved.

HTTP Proxy Filters

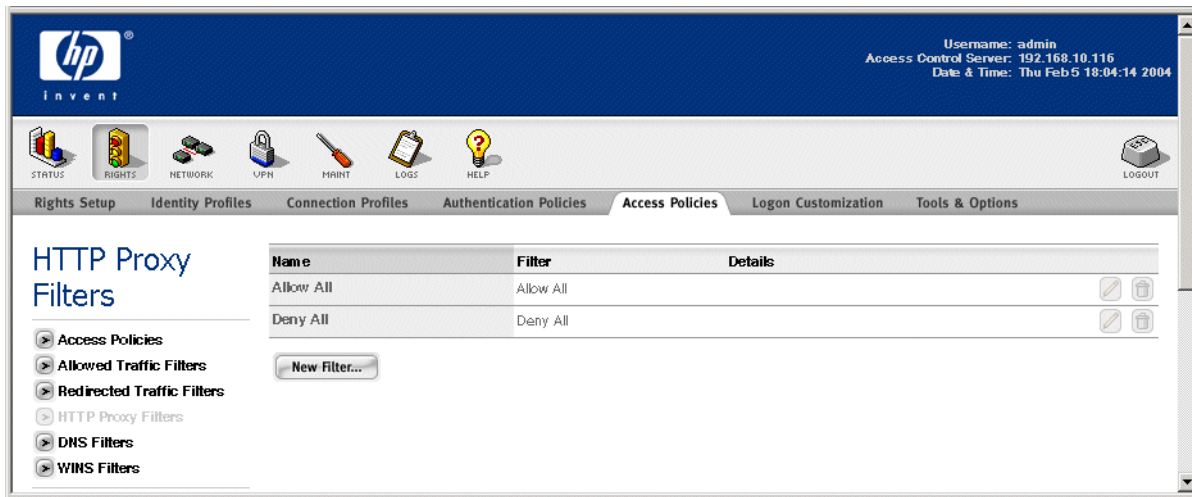
The Automatic HTTP Proxy feature of the 700w1 Series system allows you to enforce the use of an internal HTTP proxy server (within your network) without requiring a specific configuration on the client. This feature is configured as part of an Access Policy.

Within the Access Policy (under the HTTP Proxy Tab, see “The HTTP Proxy Tab” on page 4-55) you select a set of proxy filters to allow or deny HTTP traffic based on the destination of that traffic. You can select from the set of filters displayed on the HTTP Proxy Filters page.

The 700w1 Series system provides only two predefined HTTP Proxy filters—Allow All and Deny All. These are the two variations of catch-all filter that are required to be the last filter in a set of HTTP Proxy filters. You can create additional filters as needed for your specific network access requirements.

- » To view the list of HTTP Proxy Filters currently defined in the 700w1 Series system, click the **HTTP Proxy Filters** link on the main Access Policies page. The HTTP Proxy Filters page appears, as shown in Figure 4-38.

Figure 4-38. HTTP Proxy Filters List



The HTTP Proxy list shows the HTTP Proxy filters in alphabetical order, and includes the following information about each filter:

Table 4-29. HTTP Proxy Filter List Definitions

Column	Description
Name	The name for the HTTP Proxy Filter.
Filter	The type of filter.
Details	The optional description of the filter.

- » To edit a filter, click the filter name in the Name column, or click the pencil icon at the end of the row. This takes you directly to the Edit Filter: HTTP Proxy page to edit the entry for this user (see “Creating or Editing an HTTP Proxy Filter” on page 4-76).
- » To delete a filter, click the trash can icon at the end of the row.
- » To create a new filter, click the **New Filter...** button at the bottom of the filter list. This takes you to the New Filter: HTTP Proxy page (see “Creating or Editing an HTTP Proxy Filter”).

From this page you can also go directly to the Access Policies, Redirected Traffic Filters, Allowed Traffic Filters, DNS Filters or WINS Filters pages using the links directly under the page name in the left-hand panel of the page.

Creating or Editing an HTTP Proxy Filter

To create a new HTTP Proxy Filter, click the **New Filter...** button found either on the HTTP Proxy Filters page or under the HTTP Proxy tab on the New Access Policy or Edit Access Policy pages.

The New Filter: HTTP Proxy page appears (Figure 4-39) with empty fields.

The Edit Filter: HTTP Proxy Traffic page is almost identical to the New Filter page, except that the name, description, and the filter and destination definitions are displayed for the filter you have selected, and a **Save As Copy** button is provided.

Figure 4-39. Creating a New HTTP Proxy Filter

The screenshot shows the HP ProCurve management interface. At the top right, it displays 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Thu Feb 5 17:27:30 2004'. The navigation bar includes tabs for 'Rights Setup', 'Identity Profiles', 'Connection Profiles', 'Authentication Policies', 'Access Policies', 'Logon Customization', and 'Tools & Options'. The 'Access Policies' tab is selected. The main content area is titled 'New Filter: HTTP Proxy'. On the left, there are instructions: 'Enter a name and description for the filter.', 'Select a filter type from the pull-down list.', and 'In the Details field, specify the destination this filter should match. The filter type determines the format of the destination specification (IP address, FQDN, host name or regular expression). See Help for details.' Below these instructions is a 'When finished, click Save.' prompt. The form fields include: 'Name' (text input), 'Description' (text area), 'Proxy Filter' (dropdown menu with 'Allow IP' selected), and 'Details' (text area). There is a checkbox for 'Verify via DNS' and 'Save' and 'Cancel' buttons at the bottom.

To create or edit an HTTP Proxy filter, do the following:

- Step 1.** Type a name for this filter in the **Name** field. You can change the name of an existing HTTP Proxy filter by typing a new name.
- Step 2.** Type a description for the filter, or modify the existing description.
- Step 3.** In the **Proxy Filter** field, select the rule type.

An Accept rule forwards the traffic to the proxy server; a Deny rule drops the packet and redirects the client to the Stop page.

Table 4-30. HTTP Proxy Filter Types

Filter Rule Type	Description
• Allow IP	Accepts HTTP traffic destined for the specified IP address
• Allow FQDN	Accepts HTTP traffic destined for a specified fully-qualified domain name. For example, www.domain.com
• Allow Host	Accepts HTTP traffic destined for a specified host name. For example, www or home
• Allow Net	Accepts HTTP traffic destined for a specified network address (IP address and subnet mask) for example, 192.168.0.0/16

Table 4-30. HTTP Proxy Filter Types

Filter Rule Type	Description
• Allow Reg	Accepts HTTP traffic to a destination specified as a regular expression that evaluates to an address or address range For example "(.*)domain.com"
• Deny IP	Redirects HTTP traffic destined for a specified IP address
• Deny FQDN	Redirects HTTP traffic destined for a specified fully-qualified domain name For example, www.domain.com
• Deny Host	Redirects HTTP traffic destined for a specified host name For example, www or home
• Deny Net	Redirects HTTP traffic destined for a specified network address (IP address and subnet mask) For example, 192.168.0.0/16
• Deny Reg	Redirects HTTP traffic to a destination specified as a regular expression that evaluates to an address or address range. For example "(.*)domain.com"
• Allow All	Accepts all HTTP traffic. This is the alternate catch all rule The destination is always specified as "(.*)".
• Deny All	Redirects all HTTP traffic. This is the default catch all rule The destination is always specified as "(.*)".

Step 4. In the **Details** field, enter a specification for the destination that will identify the traffic that should be accepted or denied based on this rule. The description column of Table 4-30 specifies the form of the destination specifications for each filter rule type.

Step 5. 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.

Note: *The **Verify via DNS** option is a relatively costly processing operation. Therefore, it is 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.*

Step 6. Click **Save** to save this filter. If you have edited an existing filter, this replaces the original filter with the modified filter definition.

To add the modified filter as a new HTTP Proxy filter, leaving the original filter unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Filter page.

After a **Save As Copy** the same page remains displayed so you can make additional changes.

Click **Cancel** to return to the previous page without making any further changes.

Example—Modifying the “Guest Access” Access Policy

The following sections provide examples of how to modify access rights by editing the settings for an Access Policy. The Guest Access Access Policy is used as the example because you will need to modify this Access Policy (or create a copy and give it some additional rights) if you want to allow Guests users to log onto your network and have network or Internet access. The first example shows how to modify the Outside World Allowed Traffic filter to enable guest access to the Internet, but without allowing access to internal locations. The second example shows how to use the automatic HTTP proxy feature to allow HTTP access while protecting specific web sites.

By default the predefined “Guest Access” Access Policy includes only the Allowed and Redirected Traffic filters that enable a Guest to log onto the system. Once logged on, a Guest has no access rights to any part of the network or to the Internet. 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 Access Policy.

Enabling an Existing Allowed Traffic Filter—Outside World

The simplest way to modify an Access Policy is to enable or disable an existing Allowed or Redirected Traffic filter.

For example, the predefined Outside World Allowed Traffic filter allows 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 Allowed Traffic filter for the Guest Access Access Policy means that any user that logs in as a Guest will be able to access all network addresses except for those within the Access Control Server subnet.

To enable the Outside World Allowed Traffic filter for the Guest Access Policy, do the following:

Step 1. Click the **Rights** button to display the Rights Setup page (see Figure 4-40).

Figure 4-40. Selecting the Guest Access Access Policy for editing

The screenshot shows the HP ProCurve Rights Setup page. The top navigation bar includes links for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and LOGOUT. The main content area is titled 'Rights Setup' and contains a table with the following data:

Row	Identity Profile	Connection Profile	Access Policy
1	Accounting	Accounting	Accounting
2	Guest	Any	Guest Access
3	Authenticated	Any	Authenticated
4	Access Points	Any	Network Equipment
5	Any	Accounting	Unauthenticated
6	Any	Any	Unauthenticated

Below the table are buttons for 'New Rights Assignment...' and 'Refresh User Rights Now'. The 'Guest Access' link in the table is highlighted in blue, indicating it is the selected policy for editing.

Configuring Rights

Step 2. In the Access Policy column of the table, click Guest Access to display the Edit Access Policy page for the Guest Access Access Policy.

Step 3. Click the Allowed Traffic tab to display the Allowed Traffic filters currently selected for this Access Policy, as shown in Figure 4-41.

Note that the Allowed Traffic filters that are selected for this Access Policy are sorted to the top of the list.

Figure 4-41. The Allowed Traffic filters for the Guest Access Access Policy

The screenshot shows the 'Edit Access Policy' interface for the 'Guest Access' policy. The 'Allowed Traffic' tab is selected, showing a list of filters. The 'Outside World' filter is highlighted with a black arrow pointing to its checkbox.

Filter List:

Filter	Details
<input checked="" type="checkbox"/> DNS UDP 53	[Pencil icon]
<input checked="" type="checkbox"/> DNS TCP 53	[Pencil icon]
<input checked="" type="checkbox"/> AM HTTPS Logon page	[Pencil icon]
<input checked="" type="checkbox"/> DHCP	[Pencil icon]
<input checked="" type="checkbox"/> AM Stop page	[Pencil icon]
<input checked="" type="checkbox"/> AM SSL Stop page	[Pencil icon]
<input type="checkbox"/> All IP traffic	[Pencil icon]
<input type="checkbox"/> AM Logon-fwd append URI	[Pencil icon]
<input type="checkbox"/> AM Logon-fwd no URI	[Pencil icon]
<input type="checkbox"/> Appletalk	[Pencil icon]
<input type="checkbox"/> CDP and WNMP	[Pencil icon]
<input type="checkbox"/> External CS UI	[Pencil icon]
<input type="checkbox"/> HTTP	[Pencil icon]
<input type="checkbox"/> Internal Adm in UI	[Pencil icon]
<input type="checkbox"/> Internal HTTP	[Pencil icon]
<input type="checkbox"/> Internal IS UI	[Pencil icon]
<input type="checkbox"/> Internal rights UI	[Pencil icon]
<input type="checkbox"/> Kerberos	[Pencil icon]
<input type="checkbox"/> Outside World	[Pencil icon]
<input type="checkbox"/> Ping	[Pencil icon]
<input type="checkbox"/> SMB TCP 139	[Pencil icon]
<input type="checkbox"/> SMB UDP 137	[Pencil icon]
<input type="checkbox"/> SMB UDP 138	[Pencil icon]

Buttons: New Filter..., Save, Cancel

Step 4. Find the row for the Outside World filter, as shown in Figure 4-41, and click the checkbox to select the filter.

Step 5. Click **Save** to have this change take effect.

Modifying the Outside World Filter to Restrict Access


If the Outside World Allowed Traffic filter is not sufficiently restrictive for your network environment, you can modify it (or create a new filter) to restrict access to multiple subnets or IP addresses.

Step 1. From the Allowed Traffic tab, click the Outside World filter.

The Edit Filter page for Allowed Traffic appears, with the Outside World filter displayed.

Step 2. To rename this filter, type a new name in the **Name** field. To modify the Outside World filter, leave the name unchanged.

Step 3. By default, the Outside World filter allows IP traffic on any port to any destination *except* the IP address range defined by the @INTRANET@ variable.

You can view the definition of the @INTRANET@ variable by clicking the **View** button () next to the **Addresses** field.

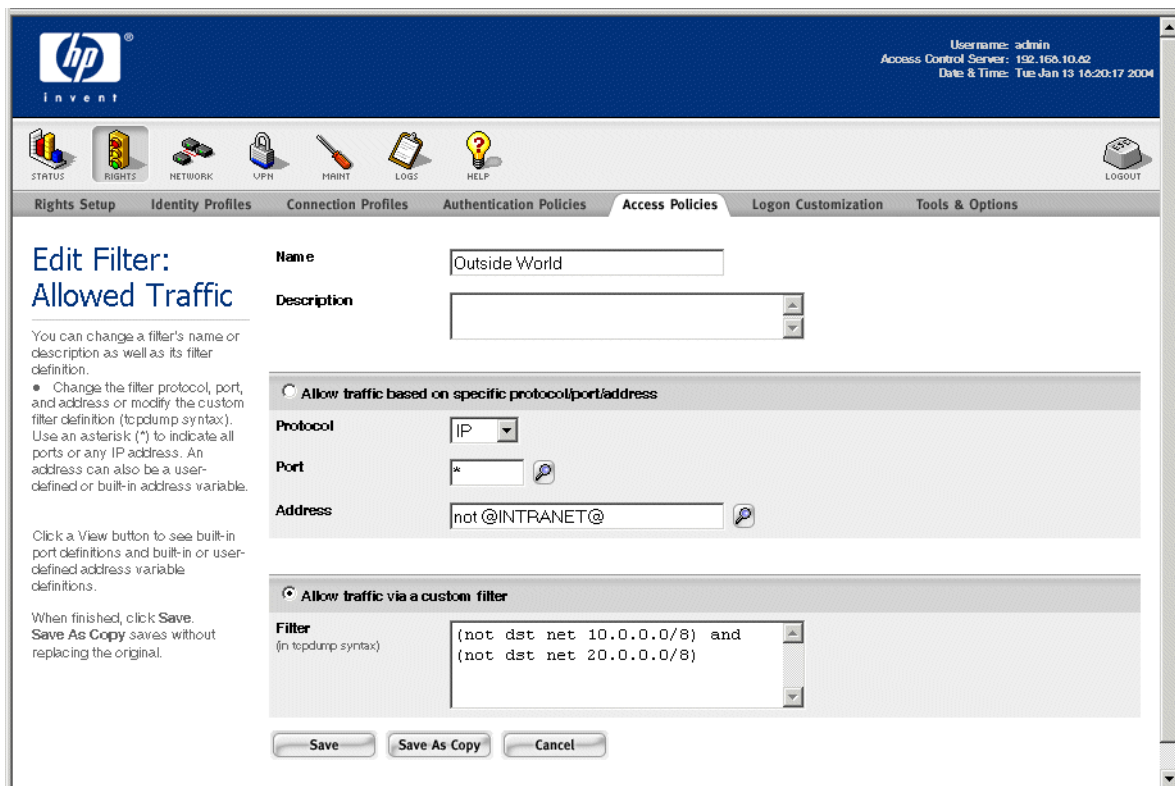
Step 4. If you want to specify a single destination IP address or address range, type it in the **Address** field. You can also create an address variable and use it here. The address can be preceded by a “!” or “not” to negate the address.

Step 5. To specify a more complicated address filter, you can enter a tcpdump expression. Select the **Allow traffic via a custom filter** radio button, and type the appropriate expression into the text box.

For example, as shown in Figure 4-42, 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)
```

Figure 4-42. Changing the Outside World Allowed Traffic filter



See [Appendix B, “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 6. If you have changed the Outside World filter, click **Save** to replace the current Outside World filter definition. To save this filter as a new filter, click **Save as Copy**.

If you have created a new Allowed Traffic filter, make sure you enable it for the Guest Access Access Policy by selecting it under the Allowed Traffic tab for the Access Policy.

Setting Up HTTP Proxy Filters

If you plan to allow guests to access your network, or to access the Internet via your network, you may want to configure the automatic HTTP proxy feature to enforce the use of an internal HTTP proxy server (within your network) without requiring a specific configuration on the client.

Note: *To use this feature, you must first configure a proxy server for each Access Controller through which Guests may access your network. This is configured under the **Network** configuration pages (see “Automatic HTTP Proxy Server Specification” on page 6-26).*

The example discussed here creates a proxy filter specification for the Guest Access Access Policy that does the following:

- Specifies that the 700wl Series system should listen for HTTP traffic on ports 3128 and 8080.
- Specifies a set of filters for HTTP traffic that allows HTTP traffic to the Internet, but denies traffic to the 192.168.x.x network and to sites at companyB.com (with the exception of two specific addresses—192.168.1.21 and www.companyB.com). The set of filters work as follows:
 - Allow HTTP traffic to the CompanyB web site at www.companyB.com.
 - Allow HTTP traffic to IP address 192.168.1.21
 - Deny HTTP traffic to all other addresses on the 192.168.x.x subnet
 - Deny HTTP traffic to any locations on companyB.com (except for www.companyB.com, which is allowed by the previous filters)
 - Allow all other HTTP traffic

To configure HTTP proxy filtering for the Guest Access Access Policy, do the following:

Step 1. Click **Rights** to display the Rights Setup page, then click the Guest Access Access Policy to display the Edit Access Policy page.

Step 2. Select the HTTP Proxy tab.

Figure 4-43 shows the HTTP proxy tab for the Guest Access Access Policy *after the set of required proxy filters have been created*.

By default, only the Allow All and Deny All filters will be present, with Deny All selected.

Figure 4-43. Configuring Proxy Filters to limit access for the Guest Access Access Policy

The screenshot shows the 'Edit Access Policy' page for the 'Guest Access' policy. The 'Allowed Traffic' tab is selected. The page contains a list of filters with checkboxes and edit buttons. The filters are as follows:

Filter	Details
<input checked="" type="checkbox"/> DNS UDP 53	
<input checked="" type="checkbox"/> DNS TCP 53	
<input checked="" type="checkbox"/> AC HTTPS Logon page	
<input checked="" type="checkbox"/> DHCP	
<input checked="" type="checkbox"/> AC Stop page	
<input checked="" type="checkbox"/> AC SSL Stop page	
<input type="checkbox"/> AC Logon-fwd append URI	
<input type="checkbox"/> AC Logon-fwd no URI	
<input type="checkbox"/> All IP traffic	
<input type="checkbox"/> Appletalk	
<input type="checkbox"/> CDP and WNMPP	
<input type="checkbox"/> External ACS UI	
<input type="checkbox"/> HTTP	
<input type="checkbox"/> Internal Adm in UI	
<input type="checkbox"/> Internal HTTP	
<input type="checkbox"/> Internal IAM UI	
<input type="checkbox"/> Internal rights UI	
<input type="checkbox"/> Kerberos	
<input checked="" type="checkbox"/> Outside World	
<input type="checkbox"/> Ping	

- Step 3.** To create the filters you need, click **New Filter....** See “HTTP Proxy Filters” on page 4-75 for details on creating HTTP proxy filters.
- Step 4.** Select **Enabled** from the drop down field to specify that filtering should be enabled. (This takes effect when you **Save** the Proxy Filter definition.)
- Step 5.** Enter the ports you want the 700wl Series system to monitor for HTTP traffic.
- Step 6.** Select and reorder (if necessary) the Proxy filters you want to use for this Access Policy. Filters are evaluated in the order that they appear in the HTTP Proxy filters list, and when a packet matches a filter, it is immediately redirected to the appropriate destination. Therefore, an incorrect ordering of HTTP Proxy filters could cause some filters never to be evaluated. In the example, the most specific filters are evaluated first, then the more general filters.
- Step 7.** Click **Save** to save the Access Policy with this set of Proxy filter specifications.

CONFIGURING AUTHENTICATION

This chapter describes how clients are authenticated through the 700wl Series system, and explains how to configure authentication policies. The topics covered in this chapter include:

Authentication in the 700wl Series System	5-1
The Rights Manager	5-4
Authentication Policies	5-4
Configuring Authentication Services	5-7
Configuring an LDAP Authentication Service	5-8
Configuring the 802.1X Authentication Service	5-16
Configuring a Kerberos Authentication Service	5-17
Configuring a RADIUS Authentication Service	5-19
Using RADIUS for Accounting	5-20
Configuring an XML-RPC Authentication Service	5-22
NT Domain Logon	5-27
External Identity Retrieval	5-28
Logon Page Customization	5-30
Tools and Options	5-42
Simulating User Rights	5-42
Tracing Authentication Service Transactions	5-47
Importing and Exporting the Rights Configuration	5-49

You can configure both Authentication Policies and Access Policies through the Rights Manager. This chapter focuses on Authentication Policies. Access Policy configuration is discussed in Chapter 4, “Configuring Rights”.

Note: *You must have Policy Administrator or Super Administrator access to perform the functions described in this chapter.*

Authentication in the 700wl Series System

The 700wl Series system grants network access rights to a client based on *who* the client is, *where* they connect to the 700wl Series system, and *when* (day, date, and time) they make the connection. The “where” and “when” are the client’s location (the Access Controller port through which it is connected) and the time window in which the connection exists. These, along with an optional VLAN tag

Configuring Authentication

specification, determine a *Connection Profile* for the client. The client's identity (who the client is) is determined through the authentication process. This is used to determine an *Identity Profile* for the client. The combination of the Connection Profile and Identity Profile determine the Access Policy that applies to the client. (See Chapter 4, "Configuring Rights" for a detailed discussion of Access Policies and access rights.)

When a client first connects to the 700wl Series system, the system attempts to match it to an Identity Profile and Connection Profile. In most cases, because it has not yet been authenticated, the client will match only the default Identity Profile ("Any"). This Identity Profile typically uses an Access Policy that allows only the access necessary to complete the logon process.

There is a "catch-all" row in the Rights Assignment Table (see "*The Rights Assignment Table*" on page 4-6) that ensures the client will always match a Connection Profile (based on the Access Controller port it connected through and the time of day) and each Connection Profile includes an *Authentication Policy* that specifies how clients connecting through that Connection Profile should be authenticated.

An *Authentication Policy* is an ordered set of one or more authentication services. An *Authentication Service* is a named instance of a particular service used for authentication, such as a specific LDAP server or RADIUS server. You configure an Authentication Service in the 700wl Series system by specifying the properties and parameters necessary to communicate with that service for the purpose of authenticating clients.

The 700wl Series system provides great flexibility in the methods it supports for authenticating users who want to log on to the network through the 700wl Series system. Users can be entered into a built-in database, their user information can be forwarded to an external authentication service, such as an LDAP server, or the 700wl Series system can be configured to accept the results of a successful VPN authentication, NT Domain logon, or 802.1x logon.

The 700wl Series system supports the following types of authentication:

- **Browser-based Logon**

Browser-based logon is the default authentication method, with the 700wl Series system built-in database as the default Authentication Service.

With browser-based logon, the user is presented with a logon page the first time she attempts to access the network with a web browser. Typically the logon page allows the user to enter a username and password. The 700wl Series system attempts to authenticate the user information through an authentication service as specified by the Authentication Policy associated with the client's Connection Profile.

For use with browser-based logon, the 700wl Series system supports the following Authentication Services:

- The Built-In Database (the default Authentication Service)
- Lightweight Directory Access Protocol (LDAP) services, including Microsoft's Active Directory and iPlanet's LDAP server.
- A Remote Authentication Dial-In User Service (RADIUS)
- A Kerberos service
- An XML-RPC-based service

You can configure one or more of these services and use them in one or more Authentication Policies. You specify the order of these services when you configure the Authentication Policy.

When the 700wl Series system receives a username and password from the logon page, the client is forwarded to the first authentication service in the list. If the first services fails to authenticate the

client, the username and password is sent to the next service, and so on. If all services in the list fail to authenticate the user, then the user will continue to have only unauthenticated logon rights.

- **Monitored Logon**

With monitored logon, the HP system passes 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.

The 700wl Series system can monitor the following logon methods:

- 802.1x
- NT Domain Logon

Both of these monitored logon methods are predefined as authentication services. You can select one or both of these methods for inclusion within an Authentication Policy.

802.1x and NT Domain logon, if selected, always take priority over any other services. If the Authentication Policy specifies either of these methods, all packets from the client are sent on to the network, and all returned packets destined for that client are “sniffed” to detect an authentication result. If the authentication is successful, the 700wl Series system re-evaluates the client to determine what rights should be granted (see “Access Rights in the 700wl Series System” on page 4-1 for a detailed explanation of how this is done). If the authentication fails, the 700wl Series system will either try the next authentication service specified in the Authentication Policy, or if no other services are defined, will continue to provide only logon rights.

Note: *NT Domain Logon does not work with clients whose IP addresses are “NAT’ed”. If you plan to use NT Domain Logon, the Access Policies associated with those clients must specify the Network Address Translation setting of **When Necessary**, but should not be set to **Always**. See “NT Domain Logon” on page 5-27 for more information about the requirements for using NT Domain logon.*

- **Wireless Data Privacy Logon**

The 700wl Series system supports a third authentication mechanism—it can accept the authentication performed by one of the Wireless Data Privacy protocols (PPTP, L2TP/IPSec, tunneled IPSec, or SSH).

Wireless Data Privacy authentication methods may involve shared secrets or certificates, and the Authentication Policy associated with the Connection Profile is not necessarily used (the Wireless Data Privacy authentication may supersede it).

- When used for authentication, SSH uses the Authentication Policy associated with the Connection Profile through which the user connected.
- L2TP and PPTP can be configured to use the Authentication Policy associated with the Connection Profile through which the user connected, or it can use a shared secret. The shared secret is configured in the Access Policy.
- Tunneled IPSec can be configured to use a shared secret or a public key certificate.

Because Wireless Data Privacy protocols are used for securing airwave traffic as well as for authentication, specification of the acceptable protocols is included in the Access Policy associated with an Identity Profile and Connection Profile pair, not the Authentication Policy. Thus, in order to use Wireless Data Privacy logon, you must ensure that the Access Policy that specifies logon rights (by default, the Unauthenticated Access Policy) is configured correctly to support the appropriate types of Wireless Data Privacy logon. See “Creating or Editing an Access Policy” on page 4-43 for details on how to configure Wireless Data Privacy logon.

The Rights Manager

The configuration of network Authentication Policies is done through the Rights module, accessed by clicking the **Rights** icon on the Navigation bar.

Many of the functions within the Rights module—specifically those associated with creating or modifying access rights through the Rights Assignment table—are discussed in Chapter 4, “Configuring Rights”. The following Rights module functions are discussed in this chapter:

- Configuring new Authentication Services (or modifying existing service configurations)
- Creating new Authentication Policies, or modifying existing policies
- Customizing the Logon page (and other associated pages) presented to users whose first network access attempt is an HTTP request.

When you have configured your Authentication Policies and made any modifications to the Logon pages, you can then use these in the specification of a Connection Profile. Creating or modifying Connection Profiles is covered in Chapter 4, “Configuring Rights”.

Authentication Policies

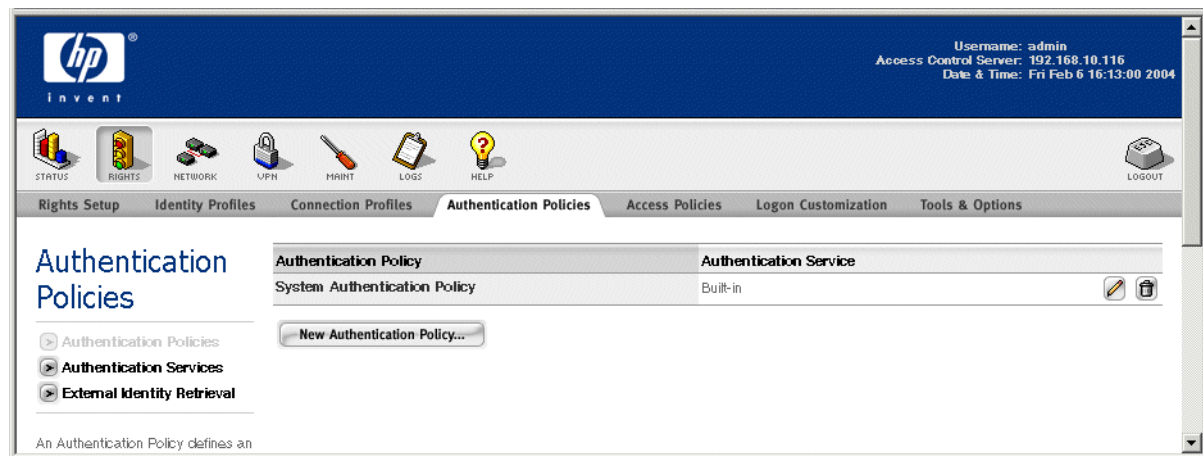
An Authentication Policy is a named, ordered set of Authentication Services. The 700w1 Series system provides one predefined Authentication Policy configured to use the built-in Authentication Service. You can include additional Authentication Services in this Authentication Policy, or you can create additional Authentication Policies.

The 700w1 Series system comes with a predefined Authentication Policy named “System Authentication Policy”. The System Authentication Policy is automatically used with all Connection Profiles unless you configure a Connection Profile to use a different Authentication Policy. If you create new Authentication Policies, you can specify which one should be considered the preferred Authentication Policy. The preferred Authentication Policy is used with any *new* Connection Profiles you create, but does not affect existing Connection Profiles.

- » To view the current Authentication Policies, click the Authentication Policies tab visible at the top of any Rights module page.

The Authentication Policies page appears (see Figure 5-1).

Figure 5-1. The Authentication Policies Page



The Authentication Policies table shows the currently defined Authentication Policies. This table shows the following information about each Authentication Policy:

Table 5-1. Authentication Policy Table Contents

Column	Description
Authentication Policy	The name of the Authentication Policy
Authentication Services	A list of the Authentication Services selected for the Authentication Policy. See "Configuring Authentication Services" on page 5-7 for information about defining Authentication Services.

- » To edit an Authentication Policy, click the Authentication Policy name in the first column of the table, or click the pencil icon at the end of the row. This takes you directly to the Edit Authentication Policy page (see "Creating or Editing an Authentication Policy" on page 5-6).
- » To edit an Authentication Service, click the name of the service you want to edit. This takes you directly to the Edit Authentication Services page for the filter you selected.

Note: You cannot edit the built-in Authentication Service or the NT Domain Logons service. For these two services, no configuration is required.

- » To delete a Authentication Policy, click the trash can icon at the end of the row.

Note: You cannot delete an Authentication Policy that is in use—an error message will inform you if this is the case. For example, you cannot delete the System Authentication Policy until you replace it with another Authentication Policy in all defined Connection Profiles.

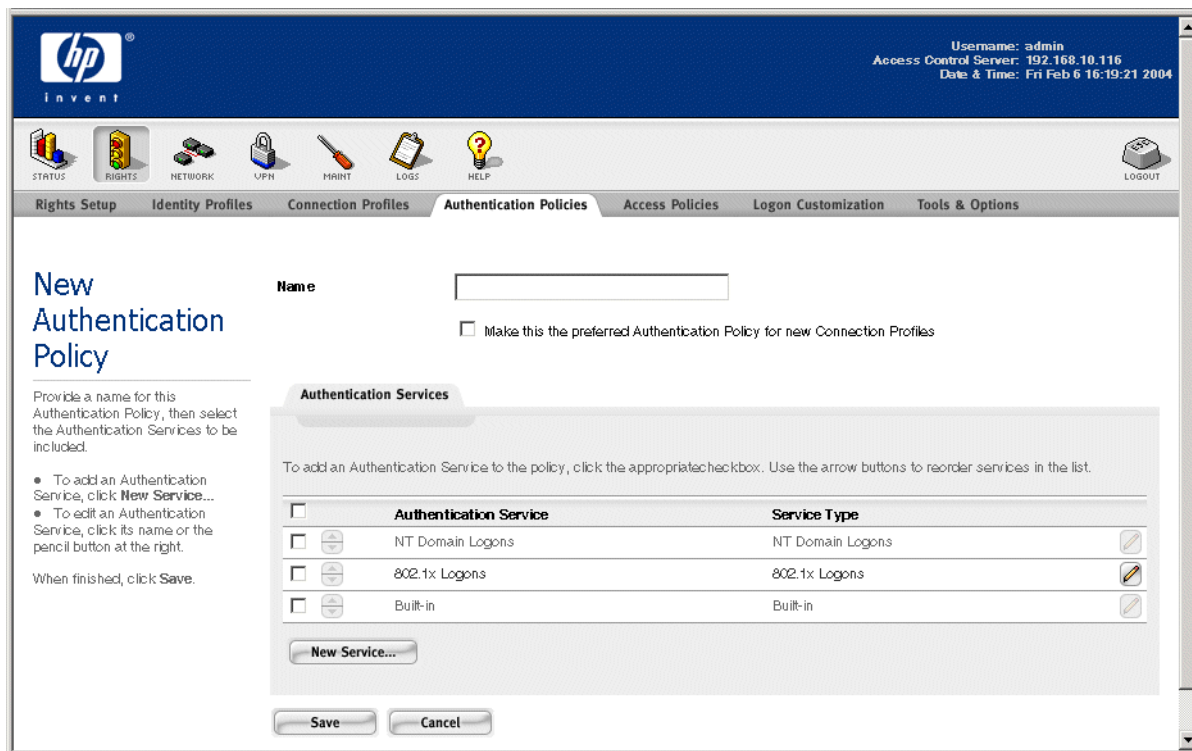
- » To create a new Authentication Policy, click the **New Authentication Policy...** button at the bottom of the Authentication Policies list. This takes you to the New Authentication Policies page.
- » To view the list of all Authentication Services, click the **Authentication Services** link under the page name in the left-hand panel of the page.

Creating or Editing an Authentication Policy

To create a new Authentication Policy, click the **New Authentication Policy...** button at the bottom of the list on the Authentication Policy page. The New Authentication Policy page appears (see Figure 5-2) with the **Authentication Services** tab initially displayed.

The Edit Authentication Policy page is almost identical to the New Authentication Policy page, except that the name and settings are displayed for the Authentication Policy you have selected. Also, a **Save As Copy** button is provided.

Figure 5-2. Creating a New Authentication Policy



To create or edit an Authentication Policy, do the following:

- Step 1.** Type a name for the policy in the **Name** field. You can change the name of an existing Authentication Policy by typing a new name.
- Step 2.** If you want this Authentication Policy to be used as the default Authentication Policy for any new Connection Profiles you create, instead of the System Authentication Policy, check the checkbox below the Name field.

Note: This does not change the Authentication Policy used in existing Connection Profiles. You must edit an existing Connection Profile to use the new Authentication Policy.

- Step 3.** Click the checkboxes of the Authentication Services you want to add to the Authentication Policy. You can select the checkbox next to the **Authentication Service** column heading to select all services in the list. Clicking this checkbox a second time removes the checks from all items in the list.

- To edit an Authentication Service, click the name of the service you want to edit, or click the pencil icon at the end of the row. This takes you directly to the Edit Authentication Services page for the filter you selected.

Note: You cannot edit the built-in Authentication Service or the NT Domain Logons service. For these two services, no configuration is required.

- To delete a Authentication Service, click the trash can icon at the end of the row.

Note: You cannot delete the NT Domain Logon, 802.1x Logon, or Built-in Authentication Services. You also cannot delete an Authentication Service that is in use—an error message will inform you if this is the case.

- To create a new Authentication Service, click the **New Service...** button at the bottom of the Authentication Services list. This takes you to the New Authentication Services page.
- To reorder a selected service in the list, click the up/down arrows to the left of the Authentication Service name.

Note: NT Domain Logon and 802.1x Logon cannot be reordered. These will always take precedence over any other authentication services.

Step 4. Click **Save** to save this Authentication Policy. If you are editing an existing Access Policy, this replaces the original Authentication Policy with the modified Authentication Policy definition.

To add the modified Authentication Policy as a new Authentication Policy, leaving the original Authentication Policy unchanged, click **Save As Copy**. The **Save As Copy** button is available only on the Edit Authentication Policy page.

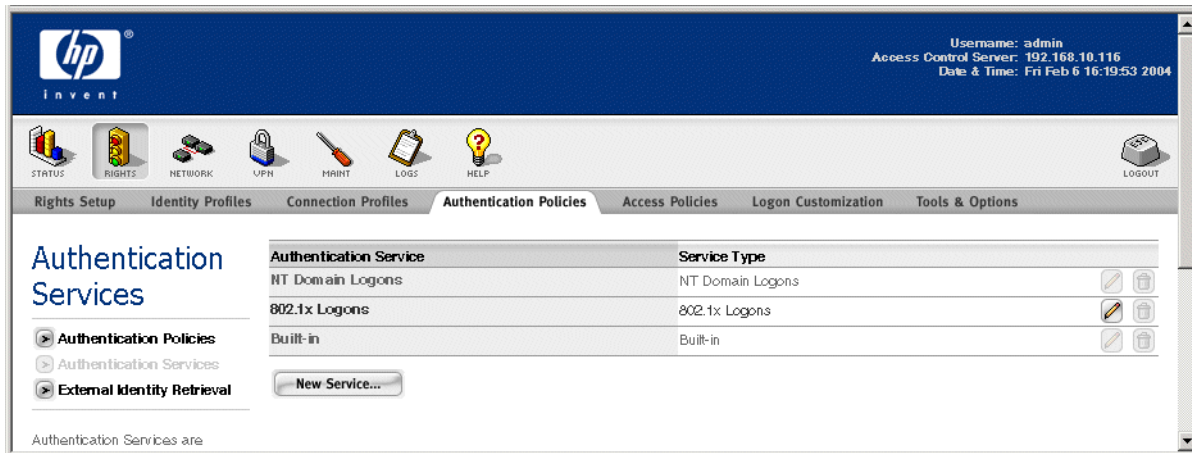
Click **Cancel** to return to the previous page without making any further changes.

Configuring 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 700wl Series system supports the following services:

- NT Domain Logon
 - 802.1x Logon
 - LDAP directory services, such as Active Directory or iPlanet LDAP server
 - RADIUS servers
 - Kerberos services
 - XML-RPC-based services
 - The 700wl Series system's built-in database. This is the default authentication service. You can populate it with usernames and passwords through the Rights module, as one of the aspects of working with Identity Profiles.
- » To view the current Authentication Services, from the Authentication Policies page click the **Authentication Services** link directly under the page name in the left-hand panel of the page. The Authentication Services page appears (see Figure 5-3).

Figure 5-3. The Authentication Services Page



The Authentication Services table shows the currently defined Authentication Services. This table shows the following information about each Authentication Service:

Table 5-2. Authentication Services Table Contents

Column	Description
Authentication Service	The name of the Authentication Service
Service Type	The type of the service

- » To edit an Authentication Service, click the Authentication Service name in the first column of the table, or click the pencil icon at the end of the row. This takes you directly to the Edit Authentication Service page (see “Configuring Authentication Services” on page 5-7).

Note: You cannot **edit** the built-in Authentication Service or the NT Domain Logons service. For these two services, no configuration is needed.

- » To delete a Authentication Service, click the trash can icon at the end of the row.

Note: You cannot **delete** the NT Domain Logon, 802.1x Logon, or Built-in Authentication Services. You also cannot delete an Authentication Service that is in use—an error message will inform you if this is the case.

- » To create a new Authentication Service, click the **New Service...** button at the bottom of the Authentication Services list. This takes you to the New Authentication Service page.
- » To view the list of all Authentication Policies, click the **Authentication Policies** link directly under the page name in the left-hand panel of the page.

Configuring an LDAP Authentication Service

To configure an Authentication Service, click the **New Services...** button at the bottom of the list on the Authentication Services or New Authentication Policy pages. The New Authentication Services page

appears (see Figure 5-4). The page initially displays the configuration options for an LDAP Authentication Service.

The Edit Authentication Service -LDAP page is almost identical to the New Authentication Service -LDAP page, except that the page and settings displayed are for the Authentication Service you have selected. Also, a **Save As Copy** button is provided. (**Save As Copy** allows you to edit an existing service and save it as a new service.)

Figure 5-4. Creating a New Authentication Service - LDAP

- » To configure a different service than the one displayed, click the appropriate link in the left-hand column of the page. This displays the configuration options for the selected service type.

Configuring Authentication

Figure 5-4 shows the configuration page for configuring an LDAP service with non-user binding. For many of the options on the LDAP service page, the values you enter are dependent on the configuration of your LDAP service, so a thorough knowledge of your LDAP implementation is necessary.

You can configure the 700wl Series system to use an external LDAP database for user authentication, and to retrieve group identity information used to associated the authenticated user with an Identity Profile. 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 700wl Series system 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 700wl Series system to bind to the directory service either anonymously, or using the root Distinguished Name (DN) and password, and retrieve the user's password. The 700wl Series system then authenticates the user.
- **User Binding** specifies that the 700wl Series system 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 bind method you select determines what fields you see on the bottom part of the LDAP configuration page.

The 700wl Series system also retrieves group identity information for the user from the LDAP server. This can be done in two ways.

- If group identity 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 identity 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 Distinguished Name 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 uses to encrypt the password
- The bind string that defines the user Distinguished Name, if you are using user binding
- The attribute that contains the group membership identity information, if it is kept in the user record
- The search string to find group membership information if it is kept in a separate record

The information required to configure an LDAP service for authentication is defined in the following tables. Table 5-3 defines the fields on the top part of the page:

Table 5-3. LDAP Authentication Configuration Options, Top Part of the Page

Field/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.
Port	The UDP Port for LDAP (default is 389)
Base DN (Distinguished Name)	The base Distinguished Name (DN) to be appended to the username.
Username Field	The name of the field (attribute) in the database that holds the username to be matched. The default is <code>uid</code> .
Group Identity Field	The 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 is retrieved after successful authentication of the user, and is used to match the user to an Identity Profile.
Additional Identity Search	The search string to use to retrieve group membership information if it is not contained in the same entry as the user information. Use <code>%s</code> in place of the actual user logon name in this string (for example, <code>cn=%s</code>). The actual user logon name is substituted for the <code>%s</code> variable.
Timeout	Authentication timeout period (in seconds), i.e., how long the 700wl Series system will wait for a response from the LDAP service before it considers the request to have failed.
Use a secure connection (SSL) (checkbox)	<p>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 700wl Series system sends the user password to the LDAP server:</p> <ul style="list-style-type: none"> • User binding • Rootdn/rootpw binding • "Use the username field as an alias..." • Password encryption set to CLEAR <p>SSL must be enabled on the LDAP server to use this option.</p>
Use LDAP v2 (checkbox)	Select this option if your Directory is based on LDAP v2. The default is LDAP v3.
Bind Method	<p>Select the bind method to be used to bind to the LDAP database:</p> <ul style="list-style-type: none"> • Select Non-User Bind if your LDAP server allows you to connect anonymously or using the root DN and root password, and you want to present a user logon and retrieve the associated user password from the directory service. • Select User Bind to bind as the user being authenticated, sending the user logon name and password to the directory service for authentication. <p>The fields in the bottom part of the page change based on this selection.</p>

Configuring Authentication

If you select **Non-user bind**, the remaining fields on the page are as follows:

Table 5-4. LDAP Authentication Configuration Options, Non-User Bind

Field/Option	Description
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 700wl Series system 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 700wl Series system can use it to authenticate the user.
Password field	The attribute that contains the user password to be retrieved. The default is the attribute <code>userPassword</code> .
Password Encryption	The method used to encrypt the password when returning it to the 700wl Series system. Select one of the following: Crypt, SHA, SSHA, MD5, SMD5, or no encryption (CLEAR). The default is Crypt. <ul style="list-style-type: none">• Crypt• SHA• SSHA• MD5• SMD5• CLEAR – no encryption
Anonymous bind	Select this to bind anonymously without a username and password. (Not all LDAP server implementations allow this option.)
Bind using rootdn/rootpw	Select this to bind using the root DN and password for the LDAP server.
Rootdn	The root Distinguished Name for your LDAP server
Rootpw	The root password for your LDAP server

If you select **User bind**, the remaining fields on the page are as follows:

Table 5-5. LDAP Authentication Configuration Options, User Bind

Field/Option	Description
User bind string	String defining the user DN for the user-level bind. String will be of the form <code>cn=%s, cn=user</code> . The actual user logon name is substituted for the <code>%s</code> 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 Distinguished Name (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.

- » For detailed instructions for setting up an Active Directory server, see “Using the Active Directory LDAP Service” on page 5-13.
- » For detailed instructions for setting up a Netscape or iPlanet server, see “Using a Netscape or iPlanet Directory Service” on page 5-14.

Using the Active Directory LDAP Service

This section guides you through the configuration choices for authenticating using Active Directory LDAP.

Step 1. Type the basic information for your Active Directory service:

- a. Type a name for this authentication service. This can be any alphanumeric string.
- b. Type the fully-qualified host name or IP address of the server where the Active Directory is located.
- c. If the LDAP server uses a port other than UPD port 389, enter the appropriate number.
- d. Type 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 components of the domain name.

For example, if your NT domain is `XYZCorp.com`, the Base DN would be:

```
dc=XYZCorp,dc=com
```

- e. In the Username field, type the name of the attribute that contains a user’s logon name. For Active Directory, this is “`sAMAccountName`”. The username is case sensitive.
- f. If you want to retrieve group information, type the Group attribute into the Group field. For Active Directory, this is the attribute “`memberof`”.
- g. The timeout value specifies the length of time the 700w1 Series system 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. You should use SSL for a secure connection, since with User Binding the 700w1 Series system sends 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 checkbox (**Use LDAPv2**) unselected.

Step 3. Select the **Bind Method** for this server:

- Select **User bind** if you are using Active Directory for user authentication (providing a username as the DN to be authenticated).
- Select **Non-user bind** if you are using Active Directory only for external group retrieval, or if you need to use aliasing because the user’s logon ID is not used as their DN. In either of these cases you must bind as the rootDN. You cannot use anonymous binding with an Active Directory service.

Configuring Authentication

To use **User binding** for authentication where the user logon ID is used as the DN, do the following:

- a. Select **User bind** from the drop-down field.
- b. Enter the following into the **User bind string** field:

```
<domain name>\%s
```

For example, for domain XYZCorp.com, this would be XYZCorp\%s.

To 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** from the drop-down field.
- b. If the user logon name is **not** the same as the DN, select the first radio button (**Use the username field as an alias...**)
- c. If the user logon name is used as the DN, select the second radio button (**Use the returned password for authentication**).
- d. Specify the field that contains the user password. Typically this will be "userPassword"
- e. Specify the encryption method. By default the Active Directory directory service uses SHA.
- f. Select **Bind using rootdn/rootpw**.
- g. Enter the **Rootdn** and **Rootpw** for your database.

Step 4. When finished, click **Save**.

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. Type the basic information about this LDAP authentication service:

- a. Type a name for this authentication service. This can be any alphanumeric string.
- b. Type 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 UDP port 389, enter the appropriate number.
- d. Type the base Distinguished Name (DN) that should be appended to the username attribute for authentication requests.
- e. Type the Username attribute (commonly "uid") that contains a user's logon name.

Step 2. If you want to retrieve group identity information to be used to match an Identity Profile, fill in the following fields:

- a. If you want to retrieve group information, specify the field that will contain the group membership information in the record to be retrieved (typically cn)
- b. Type the following string into the **Additional Identity 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 3. Specify some additional options for this LDAP server:

- a. The timeout value specifies the length of time the 700w1 Series system 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.
- b. If your LDAP server is configured to use SSL, the 700w1 Series system can use SSL to communicate with it. This is recommended if you are going to use User binding, where the 700w1 Series system sends the user password to the LDAP server. Click the first checkbox to use SSL.
- c. If your LDAP server is based on LDAP v2, click the second checkbox. By default, the 700w1 Series system assumes LDAP v3.

Step 4. 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** from the drop-down field
- 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 700w1 Series system uses the method returned in the record if it differs from the method specified in the Password Encryption field. This allows the 700w1 Series system 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 5. Click **Save**.

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 username and password, enter the configuration information specified in Table 5-3 or in the procedures detailed in the previous sections for Active Directory and iPlanet as appropriate for your LDAP server. Make sure you enter the attribute that contains a user's logon name in the **Username** field.

Configuring Authentication

Then, do the following:

- Step 1.** Because you are sending a password in the clear, make sure that you are using SSL.
- Step 2.** Select **Non-user bind**.
- Step 3.** Click the radio button labeled **Use the username field as an alias to find the user's dn and authenticate by rebinding**.
- Step 4.** 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.
- Step 5.** Click **Save**.

Configuring the 802.1X Authentication Service

802.1x authentication requires minimal configuration within the 700w1 Series system.

To configure the 802.1x service:

- Step 1.** Click the Rights button in the Navigation bar, then go to the Authentication Policies tab.
- Step 2.** Click the **Authentication Services** link in the left panel to go to the Authentication Services page.
- Step 3.** On the Authentication Services page, click **New Service...** button.
- Step 4.** Click the **802.1x** link in the left-hand panel of the page.

The Edit Authentication Service - 802.1x page appears (see Figure 5-5).

Note: There is only one configuration allowed for 802.1x authentication. Therefore, you can edit the RADIUS configuration for this service, but you cannot create a second 802.1x service.

Figure 5-5. The Edit Authentication Service - 802.1x Page

The screenshot displays the HP ProCurve Secure Access 700w1 Series Management and Configuration Guide interface. The top navigation bar includes the HP logo, the text 'invent', and user information: 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Fri Feb 6 16:21:49 2004'. Below the navigation bar is a menu with icons for STATUS, RIGHTS, NETWORK, VPN, MAINT, LOGS, HELP, and LOGOUT. The main content area is titled 'Edit Authentication Service - 802.1x' and features a sidebar with a tree view containing '802.1x', 'Kerberos', 'LDAP', 'RADIUS', and 'XML-RPC'. The main form fields include 'RADIUS Port' (1812), 'RADIUS Secret', 'Confirm RADIUS Secret', and 'Group Identity Field'. At the bottom of the form are 'Save' and 'Cancel' buttons.

Along with the authentication results, you can obtain the user's group affiliation from the authentication process. The returned group information will be used to match the user to an Identity Profile in the Rights Assignment table. This assumes you have created Identity Profiles that match the groups that may be returned from the authentication process.

Step 5. The information required to configure the RADIUS service for 802.1x authentication is defined in Table 5-6 as follows:

Table 5-6. RADIUS Configuration For 802.1x Authentication

Field/Option	Description
RADIUS Port	The port number for the RADIUS server. The default port number is 1812.
RADIUS Secret	The shared secret that allows access to the RADIUS server. This must match exactly the secret configured on your RADIUS server.
Confirm RADIUS Secret	The shared secret, entered a second time to confirm.
Group Identity Field	(Optional). The name of the attribute in the database that contains the user's group membership information. The returned group information is used to determine the Identity Profile that this user matches. If you use this option, the attribute name you enter must match a valid attribute that exists on the RADIUS server.

Step 6. Click **Save** when you have finished.

Configuring a Kerberos Authentication Service

To configure a Kerberos service, do the following:

Step 1. Click the Rights button in the Navigation bar, then go to the Authentication Policies tab.

Step 2. Click the **Authentication Services** link in the left panel to go to the Authentication Services page.

Step 3. On the Authentication Services page, click **New Service...** button.

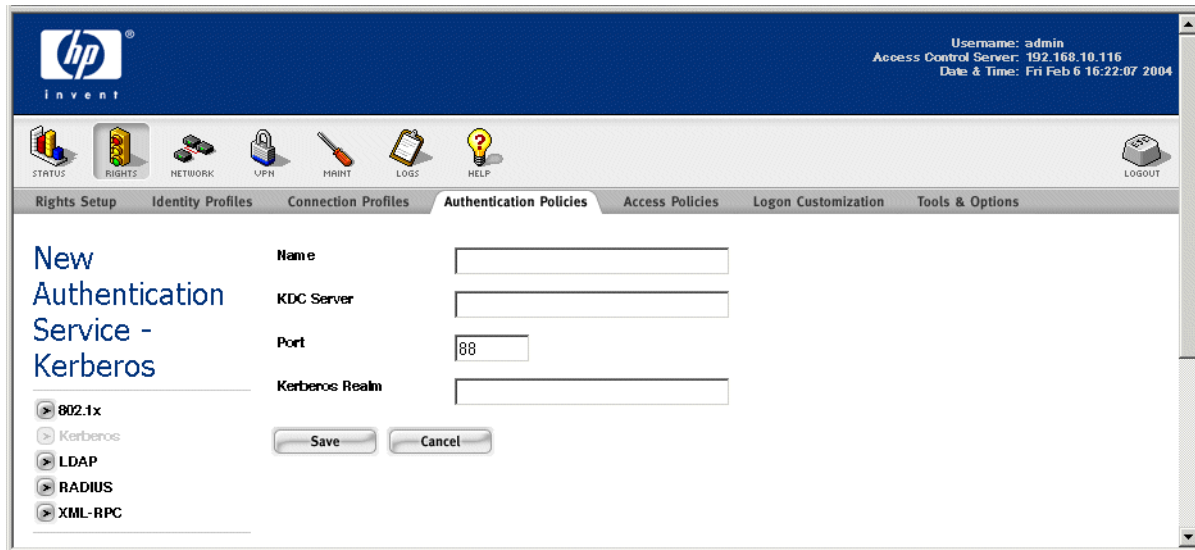
Step 4. Click the **Kerberos** link in the left panel of the page.

The New Authentication Service - Kerberos page appears (see Figure 5-6).

The Edit Authentication Service - Kerberos page is almost identical to the New Authentication Service - Kerberos page, except that the page and settings are displayed for the Authentication Service you have selected. Also, a **Save As Copy** button is provided.

Configuring Authentication

Figure 5-6. Creating a New Authentication Service - Kerberos



Step 5. Enter the information required to configure a Kerberos service for use with authentication as defined in Table 5-7:

Table 5-7. Kerberos Authentication Service Configuration

Field/Option	Description
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
KDC Server	The IP address or fully-qualified name of the server running the Key Distribution Center network service. Per RFC 1123, the KDC Server name may be a text string of up to 24 characters drawn from the alphabet (A-Z), digits (0-9), and minus sign (-). Periods (.) are allowed only when they delimit components of a "domain style name" (fully-qualified domain name).
Port	The port number used by the Key Distribution Center network service. The default is 88.
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 6. Click **Save** when you have finished.

Configuring a RADIUS Authentication Service

Note: The 700wl Series system Access Control Server must be configured as a RADIUS client on your RADIUS server.

To configure the 700wl Series system to use a RADIUS database for user authentication:

Step 1. Click the Rights button in the Navigation bar, then go to the Authentication Policies tab.

Step 2. Click the **Authentication Services** link in the left panel to go to the Authentication Services page.

Step 3. On the Authentication Services page, click **New Service...** button.

Step 4. Click the **RADIUS** link in the left-hand panel of the page.

The New Authentication Service - RADIUS page appears (see Figure 5-7).

The Edit Authentication Service - RADIUS page is almost identical to the New Authentication Service - RADIUS page, except that the page and settings are displayed for the Authentication Service you have selected. Also, a **Save As Copy** button is provided.

Figure 5-7. Creating a New Authentication Service - RADIUS

The screenshot displays the 'New Authentication Service - RADIUS' configuration page. At the top, the HP logo and 'invent' tagline are visible. The page header shows the user is logged in as 'admin' with IP '192.168.10.116' on 'Fri Feb 6 16:22:13 2004'. A navigation bar contains icons for STATUS, RIGHTS, NETWORK, VPM, PRINT, LOGS, HELP, and LOGOUT. Below this is a tabbed interface with 'Authentication Policies' selected. The main form area is titled 'New Authentication Service - RADIUS' and includes a list of authentication protocols: 802.1x, Kerberos, LDAP, RADIUS (selected), and XML-RPC. A text box explains that for RADIUS, a name and required information must be provided. The form fields are: Name (empty), Server (empty), Port (1812), Secret (empty), Confirm Secret (empty), Group Identity Field (empty), Reauthentication Field (Session-Timeout), and Timeout (5 seconds). There are two checkboxes: 'Supports Microsoft Attributes (RFC-2548)' (unchecked) and 'Enable RADIUS Accounting (RFC-2866) on port 1813' (unchecked). 'Save' and 'Cancel' buttons are at the bottom.

Along with the authentication results, you can obtain the user's group affiliation from the authentication process. The returned group information will be used to match the user to an Identity Profile in the Rights Assignment table. This assumes you have created Identity Profiles that match the groups that may be returned from the authentication process.

Configuring Authentication

The information required to configure the RADIUS service for authentication is defined in Table 5-8 as follows:

Table 5-8. RADIUS Authentication Service Configuration

Field/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.
Port	UDP Port for RADIUS (Default is 1812).
Secret	The shared secret for this RADIUS server.
Confirm Secret	The shared secret, entered a second time to confirm.
Group Identity Field	The RADIUS attribute that contains Identity Profile membership information.
Reauthentication Field	The name of a RADIUS attribute that contains a time specification (in seconds) used to force periodic user reauthentication. The default attribute is Session-Timeout. For example, if the value retrieved from this field is 7200 seconds (2 hours) all users will be forced to reauthenticate every 2 hours.
Timeout	Authentication server request timeout (in seconds). If the RADIUS server has not completed the authentication requests within this interval, the authentication is considered to have failed.
Enable RADIUS Accounting (RFC 2866)	Check this to enable RADIUS accounting support using this RADIUS server. The RADIUS server must support RFC 2866. See "Using RADIUS for Accounting" on page 5-20 for more details about the RADIUS accounting feature.
on Port	UDP port for RADIUS accounting (Default is 1813).
Supports Microsoft's attributes (RFC 2548)	Check this to indicate that the RADIUS server supports Microsoft vendor-specific RADIUS attributes, including MSCHAP. Note: You must check this if you will use this RADIUS server to authenticate PPTP or L2TP sessions.

Step 5. Click **Save** when you have finished.

Using RADIUS for 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 client's activity session about the resources (time, packets, bytes etc) that were used during that session. An activity session in this context is the period between when the client logs on to or roams to the Access Controller, and when the client leaves the Access Controller, by logging off or roaming away.

You can use RADIUS accounting either in addition to or independently of using RADIUS for authentication. When you set up RADIUS as an Authentication Service, you can specify that it also be used for accounting. If you did not enable the accounting feature when you initially set up the RADIUS Authentication Service, you can modify the Authentication Service to enable RADIUS accounting. You can also create a RADIUS Authentication Service specifically to use for accounting.

- » To use a RADIUS service for accounting, you must configure a RADIUS server as an Authentication Service, and check the **Supports RADIUS Accounting (RFC-2866) on port** checkbox and enter the appropriate port number to which the 700wl Series system should send the accounting data.

Specifying a NAS-ID for Use with RADIUS Accounting

The RADIUS accounting server expects to receive a NAS-ID — the name of the RADIUS client (the Access Controller) that sent the accounting information— as part of the accounting information that it receives. By default, if no NAS-ID is set, the 700wl Series system 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.

You can specify a NAS-ID by editing the Access Controller from the System Components tab in the **Network** area. Select the Access Controller from the System Components List and type a description in the NAS-ID/Description field (see “Configuring Access Controllers” on page 6-10).

Accounting Packet Data

The following fields are sent to the RADIUS Accounting server in the accounting Start packet sent at the start of a client activity session. This information is sent whenever a an authenticated client is newly associated with an Access Controller, either due to the original logon event, or to a roaming event.

Field	Data
User-Name	The username (logon 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 client session

The following fields are sent to the RADIUS Accounting server in the Stop accounting packet sent at the end of a client’s activity session on the Access Controller, due to the client being logged off, or to roaming away from the Access Controller.

Field	Data
User-Name	The username (logon name)
NAS-IP-Address	IP address of the through which Access Controller the client is connected
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

Configuring Authentication

Field	Data
Acct-Session-ID	The unique ID for this client session
Acct-Session-Time	The seconds this client was logged on this Access Controller. Sent only with a Stop packet.

Note: When an authenticated client roams to a new Access Controller, a Stop packet is sent upon disassociation from the first Access Controller, and a Start packet is sent upon association with the new Access Controller.

Configuring an XML-RPC Authentication Service

The 700w1 Series system 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 700w1 Series system acts as an XML-RPC client, and communicates with an XML-RPC service through HP's XML-RPC Remote Profiles API.

Setting up the 700w1 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 HP 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" on page 5-24. For more information on developing the XML-RPC service, see "The XML-RPC Service" on page 5-24.
- You must configure the Rights Manager to send authentication requests to an XML-RPC server. This is discussed in this section.
- Through the Rights Manager you must create Identity Profiles that match each group that can be returned in a user profile. See "Creating or Editing an Identity Profile" on page 4-13 for an explanation of how to create Identity Profiles. The Identity Profile name must match the returned group name exactly.

Depending on the rights you want to grant to users, you may also need to create Access Policies to be associated with these Identity Profiles in the Rights Table.

Once the XML-RPC authentication service has been configured, the authentication and authorization process works as follows:

- When a new user (client) connects to the 700w1 Series system, the system presents a logon page, and retrieves the client's user identification information, including username, password, the client's MAC address and the Access Controller Location through which he/she connected.
- The 700w1 Series system 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 (username, 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 "user profile" that specifies the groups to which the user belongs, and a start and stop time for each group.

- The Rights Manager uses the group information and the start and stop times from the user profile to temporarily map the user to a matching Identity Profile, during the timeframe defined by the stop and start times in the profile. At other times (outside the range defined by the start and stop times) the user will not match that Identity Profile.

For example, suppose a user profile returns a group "GroupA" with a start time of 10:00 AM and a stop time of noon, Monday through Friday. Based on this user profile, the user will match the Identity Profile "GroupA" between 10:00AM and noon every weekday, and will get access rights based on the Access Policy that's associated with that Identity Profile in the Rights Table. At any other time of day, and on weekends, the user will not match Identity Profile "GroupA" and will not have the rights associated with that Identity Profile.

The current implementation of the XML-RPC 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" on page 5-24.

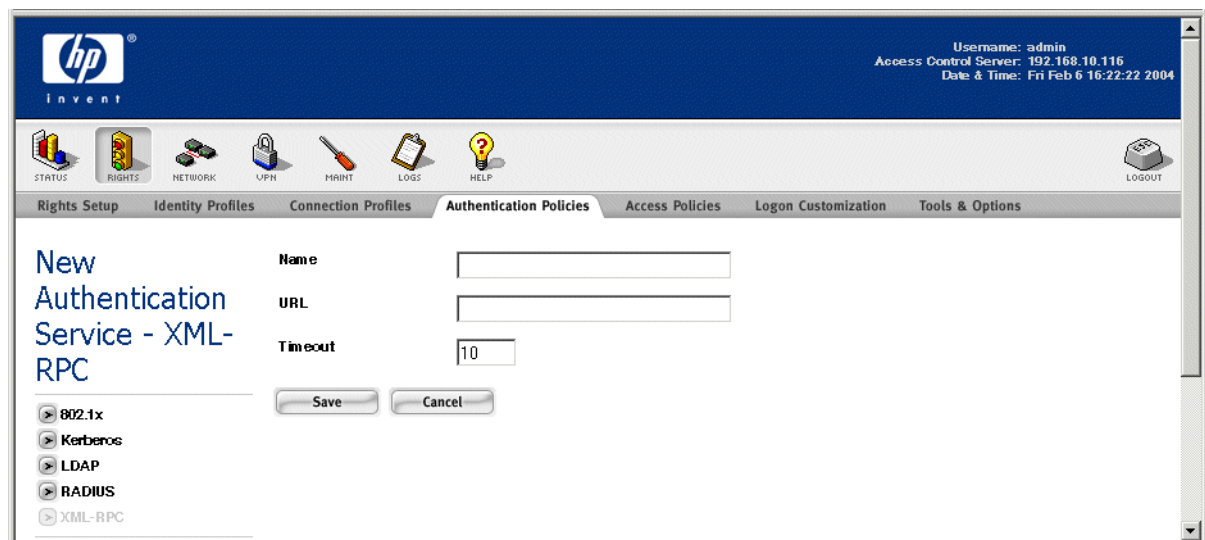
To configure the 700wl Series system to use an XML-RPC service for user authentication:

- Step 1.** Click the Rights button in the Navigation bar, then go to the Authentication Policies tab.
- Step 2.** Click the Authentication Services link in the left panel to go to the Authentication Services page.
- Step 3.** On the Authentication Services page, click **New Service...** button.
- Step 4.** Click the **XML-RPC** link in the left-hand column of the page.

The Create Authentication Service - XML-RPC page appears (see Figure 5-8).

The Edit Authentication Service - XML-RPC page is almost identical to the New Authentication Service - XML-RPC page, except that the settings are displayed for the Authentication Service you have selected. Also, a **Save As Copy** button is provided.

Figure 5-8. Creating a New Authentication Service - XML-RPC



Configuring Authentication

The information required to configure an XML-RPC authentication service is defined in Table 5-9 as follows:

Table 5-9. XML-RPC Authentication Service Configuration

Field/Option	Description
Name	Your name for this authentication method. You can use any alphanumeric string as the name.
URL	The URL of the XML-RPC service to which authentication requests should be sent.
Timeout	Authentication request timeout (in seconds). If the XML-RPC service has not completed the authentication requests within this interval, the authentication is considered to have failed.

Step 5. Click **Save** when you have finished.

The XML-RPC Service

The XML-RPC authentication service required by the 700w1 Series system is a piece of code that sits on the remote system between the 700w1 Series system Remote Profiles API and whatever system (database, directory, or application) is used to contain user authentication and scheduling information.

The XML-RPC authentication service must perform the following tasks:

- The XML-RPC service accepts an “authenticate” <methodCall> from the 700w1 Series system Rights Manager.
- The service extracts the user identification information, and constructs the appropriate inquiry needed to authenticate the user and retrieve his or 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.
- 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>.

The Remote Profiles API

The Remote Profiles API consists of a single call/response pair. The 700w1 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. 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 700w1 Series system, in turn query the appropriate database, and then form and send the appropriate response.

The authenticate call to be made by the 700w1 Series system is defined as follows:

```
authenticate (userid, password, location, MAC, options, randomstring)
```

These parameters are shown in Table 5-10:

Table 5-10. Parameters for Authenticate Call

Parameter	Type	Description
userid	string	User logon from 700wl Series system logon page
password	string	Password from 700wl Series system logon 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 <code>auth_profile</code>
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>easyPwd</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 5-11:

Table 5-11. Name/value Pairs Returned by Authenticate Response

Name	Type	Value and Description
userid	string	User logon from HP logon page, as passed in authenticate request
authenticate_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:
profileName	string	A name that matches a 700wl Series group name

Table 5-11. Name/value Pairs Returned by Authenticate Response

Name	Type	Value and Description
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 <code>hh:mm:ss</code> that defines the time of day at which these rights should take effect
stopTime	string	Time in the format <code>hh:mm:ss</code> 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 <code>YYYY-MM-DD</code> that defines the day of the year on which these rights should take effect
stopDate	string	Day of the year in the format <code>YYYY-MM-DD</code> 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>

```

NT Domain Logon

NT Domain logon requires that the 700wl Series system be able to monitor (or “sniff”) packets going between an unauthenticated client (or reauthenticating client) and the network. When the 700wl Series system detects that a successful authentication has occurred, it then provides access rights based on the Access Policy associated with the Connection Profile and Identity Profile that apply to that client.

NT Domain logon does not require configuration as an Authentication Service within the 700wl Series system. You simply need to include it as a selected service in the appropriate Authentication Policy. However, there are a number of considerations when using NT Domain Logon for authentication.

NT Domain logon does not work with clients whose IP addresses are NAT’ed. If you plan to use NT Domain Logon, the following conditions apply:

- You must have an external DHCP server available to provide real IP addresses for your clients. See “Network Communication—the Basic Setup Tab” on page 6-19 for more information.
- Access Policies associated with those clients must specify the Network Address Translation setting of **When Necessary** (see “Creating or Editing an Access Policy” on page 4-43 for more information).
- In Access Policies associated both with unknown and authenticated clients that use NT Domain logon, the appropriate Allowed Traffic filters must be enabled, depending on the type of traffic used for the organization’s Microsoft Domain implementation:
 - The Kerberos Allowed Traffic filter
 - The SMB Allowed Traffic filters (SMB 137, SMB 138, and SMB 139)
 - An Allowed Traffic filter to allow (`dst port 389`) for LDAP.

The Kerberos and SMB Allowed Traffic filters are predefined, and are enabled in the Unauthenticated Access Policy, which is the default policy for unknown clients. These must be

Configuring Authentication

enabled in any other Access Policies that may be in force when a client is required to reauthenticate.

The Allowed Traffic Filter for LDAP must be created and then enabled in the appropriate Access Policies.

Note: *Cached Logon requests from Windows clients are not supported because the 700wl Series system cannot reliably detect a logon in a cached request. To the client, the logon will appear to succeed, but the 700wl Series system will consider the client to be unauthenticated. If this is a problem, disable cached logon through the Windows registry on the client. Go to*

MY Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon and set CachedLogonsCount to "0".

Identity Profiles and NT Domain Membership

Users who are authenticated using NT Domain Logon can be associated with an Identity Profile based on the NT Domain under which they were authenticated. To accomplish this, you must create an Identity Profile whose name matches exactly the name of the domain. Users that authenticate under that domain will then automatically be associated with the Identity Profile of the same name, and you can specify an appropriate Access Policy based on the Identity Profile.

When using the monitored NT Logon feature with an Active Directory enabled Microsoft server (Windows 2000 Server, 2003 Server, etc.) two Identity Profiles must be created matching both the SMB and the FQDN (Fully Qualified Domain Name) version of the Microsoft domain name, if a correlation between a Microsoft domain and a 700wl Series Identity Profile is desired. Each of these Identity Profiles should use the same Access Policy in the Rights Assignment Table to define access rights for users that match the Identity Profile.

Microsoft maintains both SMB and FQDN domain names on their Active Directory enabled servers in order to maintain full backwards compatibility with legacy Windows clients. Moreover, Microsoft clients will, at times, send logon requests containing the SMB version of the domain, and, at other times, send logon requests containing the FQDN version of the domain. Consequently, the creation of both of these Identity Profiles accommodates the existence of both of these names.

External Identity Retrieval

With most of the Authentication Services supported by the 700wl Series system, group identity information can be retrieved along with a successful authentication. The group identity information is used to match the user to an Identity Profile. However, if the service you use for authentication does not provide group identity information, it is possible to retrieve group identity information from an LDAP service, post-authentication, in a second operation. The retrieved group identity is used to automatically associate the user with the Identity Profile of the same name, and you can specify an appropriate Access Policy based on the Identity Profile.

Note that you must have Identity Profiles configured that match exactly the group identity names that can be retrieved from the external LDAP service.

For example, suppose you elect to use 802.1x authentication against a RADIUS service that does not maintain group information for its users, but you also have an LDAP service available that does maintain that information. In this case you could retrieve group identity information from the LDAP directory service for each user that is successfully authenticated.

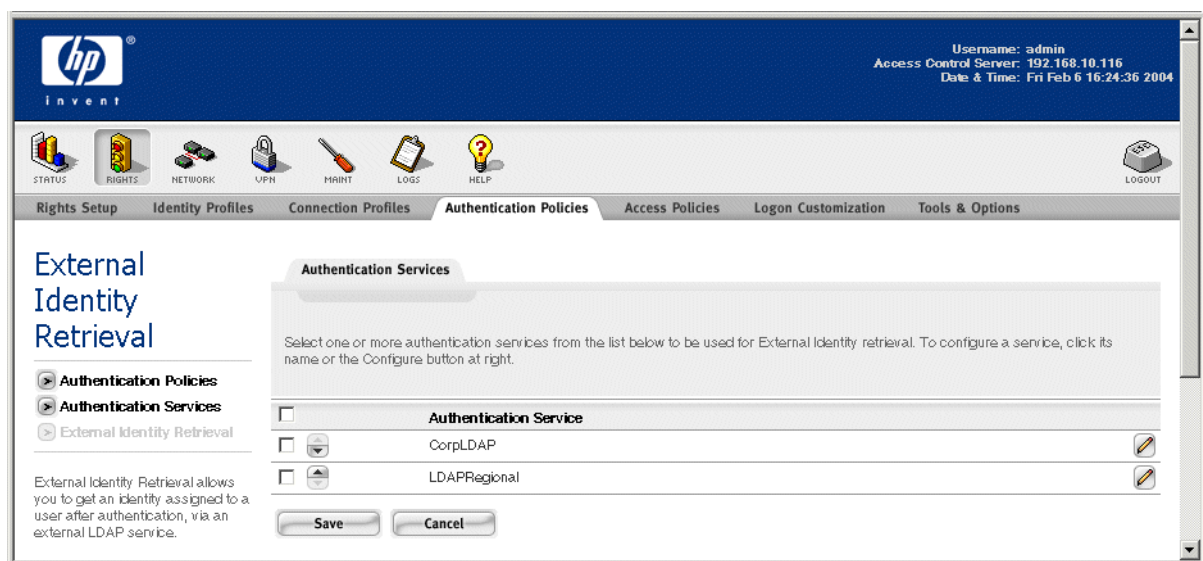
Setting up post-authentication group identity retrieval involves two procedures:

- First, you must configure an LDAP Authentication Service to be used to retrieve the group identity 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” on page 5-8 for details on how to set up an LDAP service.
- Second, you specify the LDAP service(s) you want to use for group identity retrieval.

To set up post-authentication group identity retrieval from an external LDAP service, do the following:

Step 1. Under the Authentication Policies tab in the Rights Manager, click the External Identity Retrieval Link in the left panel of the page. This displays the External Identity Retrieval page, as shown in Figure 5-9.

Figure 5-9. External Identity Retrieval



If there are any LDAP Authentication Services configured with Non-User Binding, they are displayed in this list.

If no eligible services exist, the list is empty. You can use the Authentication Services link in the left panel to go to the Authentication Services page and create or edit an Authentication Service.

Step 2. Select from the list the services you want to use to retrieve a group identity information.

If external group retrieval is configured, each time a user is authenticated a second request is made to the LDAP service to retrieve the group identity for the user. You must ensure that you have configured the LDAP Authentication Service to return the correct group information for these users. You can click an Authentication Service name to edit its configuration.

Step 3. If you select multiple services to be searched for group identity information, they are searched in the order they appear in the list. Use the up/down buttons at the left of the service names to reorder the services in the list.

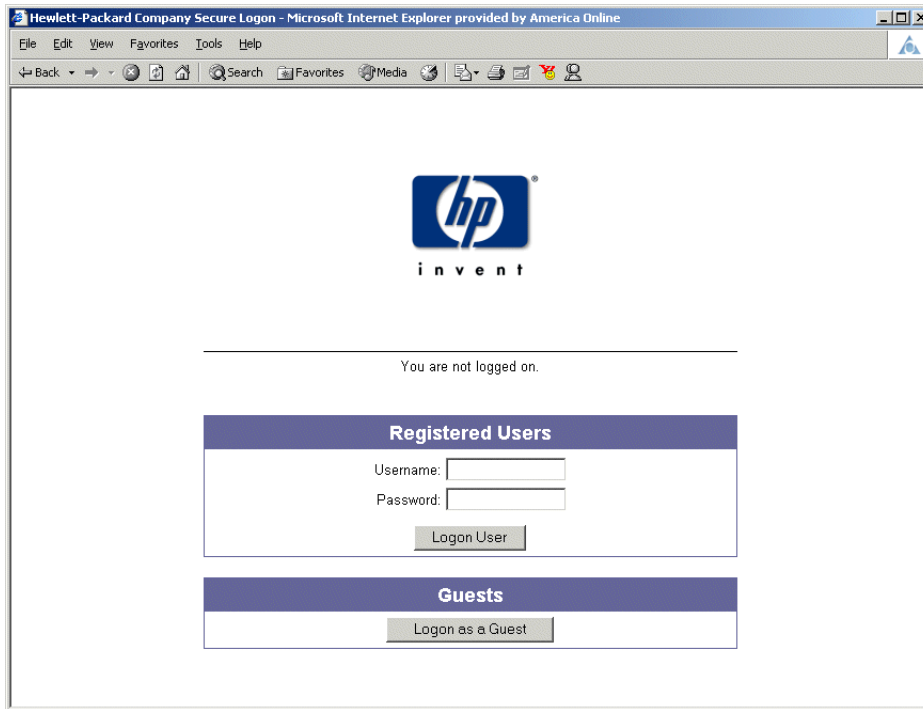
Step 4. Click **Save** when you have finished.

Once you have configured External Identity Retrieval, it will operate automatically as part of the authentication and rights assignment process.

Logon Page Customization

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 ProCurve logo, and appears as shown in Figure 5-10.

Figure 5-10. The default Logon page



Through the Rights Manager in the Administrative Console, 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 via the appropriate Connection Profile within the organization. If you use multiple Authentication Policies (for example, a Business School Authentication Policy and a Medical School Authentication Policy) you can optionally allow the user to choose the appropriate Authentication Policy.

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 built-in database, and are associated with the Guest Identity Profile. Once registered, a registered guest can log on again using their username and password, and are therefore considered authenticated users when they log on to the system. As long as the Guest Identity Profile occurs in the Rights Assignment table prior to the default Authenticated Identity Profile, registered guests will match the Guest Identity Profile and will have only Guest access rights.

Note: If the default Authenticated Identity Profile occurs in the Rights table prior to the Guest Identity Profile, registered Guests will match the Authenticated Identity Profile and will receive rights based on the Access Policy associated with the Authenticated Identity Profile.

Through the Rights Manager, you can customize the appearance of the Logon, Logoff and Stop pages in the following ways:

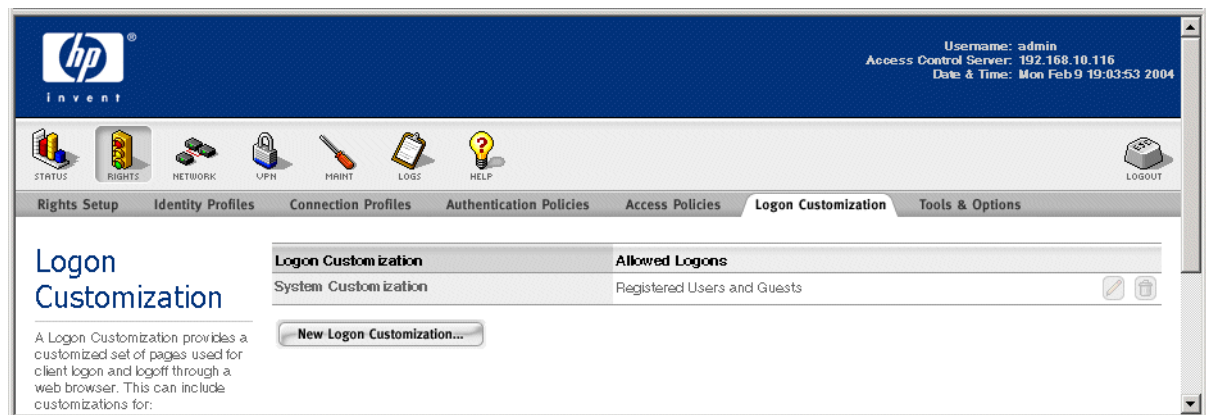
- You can create customized versions of the standard Logon, Logoff and Stop pages by including your own text and logos.
- You can associate a different customized page for each Connection Profile you have created in the Rights Manager.
- You can specify whether Guest logon should be allowed for this Connection Profile, and whether Guest users should be required to go through a registration process.
- 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 Logon Customization page, do the following:

Step 1. From anywhere within the Rights Manager, click the **Logon Customization** tab.

The Logon Customization page appears, showing the current list logon pages, as shown in Figure 5-11.

Figure 5-11. The Logon Customization Page



From the Logon Customization page you can create:

- » Click **New Logon Customization...** to create a new Logon Customization page.
- » Click the pencil icon (✎) in the row of an existing Logon Customization page to modify that page. There is a default Logon Customization page. This cannot be edited or deleted.
- » Click the trash can icon (🗑) in the row of an existing Logon Customization page to delete that page.

Note: You cannot delete a Logon Customization page that is configured for use in a Connection Profile.

Customizing a Logon Page

To create a new logon customization page, do the following:

Step 1. From anywhere within the Rights Manager, click the **Logon Customization** tab.

Step 2. Click **New Logon Customization...**

The New Logon Customization page appears, as shown in Figure 5-12.

Step 3. Enter the name you wish to give this Logon Customization page.

The name may include only characters that are valid in a file name: a-z, A-Z, 0-9, . (period), #, - (dash), _ (underscore) and the space character.

Step 4. If you wish to make this Logon Customization page the default logon page for all future Connection Profiles, put a check mark in the **Make this the preferred logon customization for new Connection Profiles** checkbox.

Step 5. To save this Logon Customization page, click **Save**.

The Logon Customization page you have created will be saved with the name you have given it. If this is all you do, the page will have the default format. You can customize your new Logon Customization page when you create it, or you can edit it later to add custom graphics and text, or you can do both.

Figure 5-12. New Logon Customization Page

hp
invent

Username: admin
Access Control Server: 192.168.10.116
Date & Time: Mon Feb 9 15:35:48 2004

STATUS RIGHTS NETWORK UPN MAINT LOGS HELP LOGOUT

Rights Setup Identity Profiles Connection Profiles Authentication Policies Access Policies **Logon Customization** Tools & Options

New Logon Customization

Logon page customization may be accomplished in two ways:

- Under **Settings** provide new images and text to be used with the standard Logon, Logoff and Stop pages.
- Under **Custom Templates** provide customized HTML template files to replace the standard pages.

Reset to Defaults resets all field values to system defaults. Click **Save** to save the contents of the tab.

Note: Unsaved changes are lost when you switch tabs.

Check **Make this the preferred customization** to have this be the default selection when creating a Connection Profile.

Name

Make this the preferred Logon Customization for new Connection Profiles

Settings Custom Templates

Provide an image file name and URL to customize the logo for the Logon and Logoff pages. Enter text and select the appropriate logon options to customize the Logon page. Provide an image and text to customize the Stop page. See **Help** for further explanation.

Logos

Logo

Small Logo

Logo URL
(Link logos to this address)

Logon Page

Logon Page Text

Allowed Logons

Allow users to specify authentication policies
 Require guests to register before logging on
 Display logoff window after logging on

Stop Page

Stop Page Image

Stop Page Text

Customizing the Logo

In the **Logos** section of the New/Edit Logon Customization page you can customize the logo (image) that appears on the logon and logoff web pages. The filename of the current logo is displayed underneath the filename entry field for the logo, along with the date that the logo was uploaded to the Rights Manager. The HP logo is the default logo.

You can use two different logos, a standard logo and a small logo. For clients with small browser screens, such as PDAs or mobile phones, the Rights Manager provides a **Small Logo** more appropriate to the size

Configuring Authentication

of a small screen. You can change this logo to be a small version of your own logo for use with small browsers.

To change either logo, do the following:

Step 1. Go to the Logos section of the New/Edit Logon Customization page and select the logo you wish to change.

Step 2. In either the **Logo** or the **Small Logo** field, type the full path and name of a file, on your local system, format that contains the logo you want

or

Click **Browse** to locate the proper directory and file name.

This file can be a GIF, JPEG, or PNG file, or any other browser-compatible graphic file format.

Step 3. You can link the logo to a URL (for example, your organization's corporate web site) so that a user can click on logo on the logon page to go to your site. Enter the appropriate URL in the **Logo URL** field provided, this should include the "http://" prefix.

The default URL is `http://www.hp.com/go/hpprocurve`.

Step 4. Click **Save** at the bottom of the page to save these changes.

Click **Cancel** to abandon any changes you have made without saving them.

To restore the default logo, click **Reset to Defaults** at the bottom of the page.

Note: *Clicking Reset to Defaults will reset all the settings for this Logon Customization page (and the associated stop page) to the default settings.*

Customizing the Logon Page Text

You can add text to a Logon Customization page with any text and HTML formatting commands you want displayed on the Logon Customization page.

To add or edit text for the Logon Customization page:

Step 1. Go to the **Logon Page** section of the New/Edit Logon Customization page, as shown in Figure 5-12.

Step 2. In the textbox labeled **Logon Page Text** enter the text you want to display to the logon user. This can include HTML formatting commands.

Step 3. Click **Save**.

To clear the logon page text after it has been set, click **Reset to Defaults** at the bottom of the page.

Note: *Clicking Reset to Defaults will reset all the settings for this Logon Customization page (and the associated stop page) to the default settings, not just the logon page text.*

You can also change several Logon Page Options:

Step 1. You can specify who is allowed to logon through this logon page. Choose either **Registered Users and Guests**, **Registered Users only**, or **Guests only**. These settings determine whether the **Logon User** button or the **Logon as Guest** button, or both buttons, appear on the page, allowing such logons, as shown in Figure 5-13.

Step 2. Place a check mark in the **Allow users to specify authentication policies** checkbox if you want users to choose a specific Authentication Policy from a group of Authentication Policies. When this option is checked, the Logon page will display a drop-down field that will allow a user to select from the Authentication Policies configured for the 700wl Series system. For example, in a University users could choose the Business School Authentication Policy or the Medical School Authentication Policy.

Step 3. To require Guest users to go through a registration process, place a check in the **Require guests to register before logging on** checkbox.

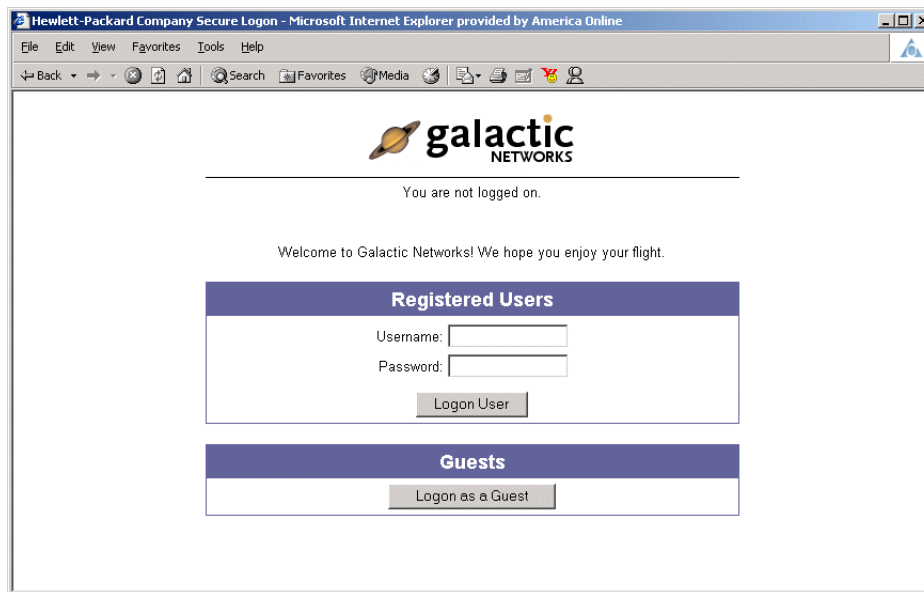
If you choose this option, the Logon as Guest button is replaced by a **Register as Guest** button, and the Guest user is taken to a registration page, as shown in Figure 5-14.

Step 4. Click **Save**.

You can also have the system display a logoff page when users log onto the system, see “Logoff Page Option” on page 5-36.

Figure 5-13 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 Policy, and the guest registration option.

Figure 5-13. Customized Logon Screen



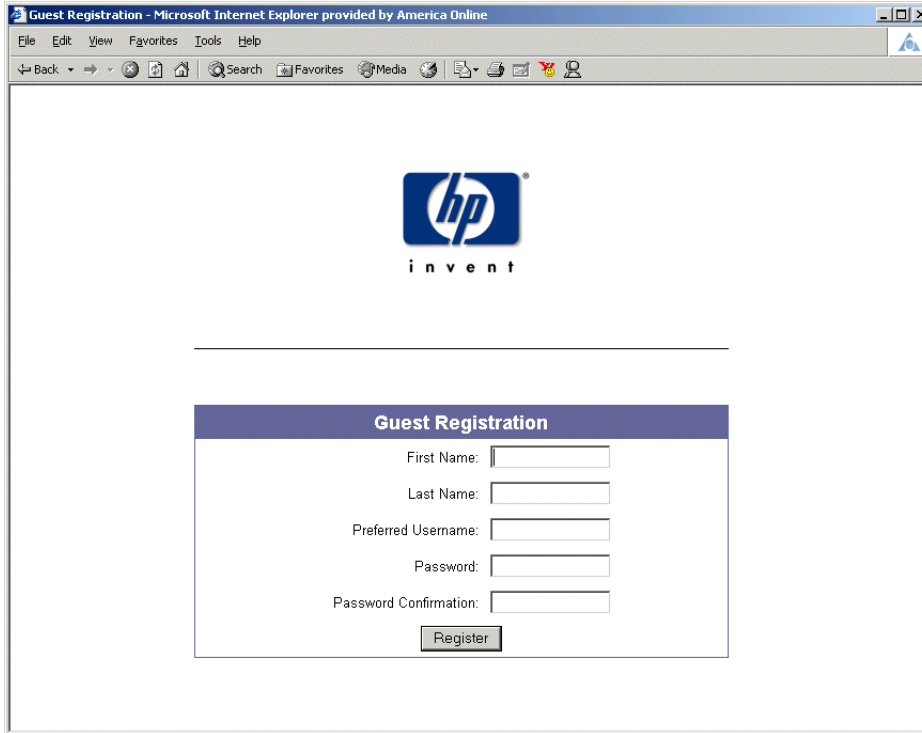
Guest Registration

Note: Regular Guest users (non-registered) are not considered authenticated when they log in. However, Registered Guests are considered authenticated as they match a username and password in the built-in database. As long as the Guest Identity Profile appears in the Rights table **prior** to the default “Authenticated” Identity Profile, registered guests will match the Guest Identity Profile and will receive only Guest rights, but if the “Authenticated” Identity Profile occurs first, registered Guests will match it and receive rights based on the Access Policy associated with the Authenticated Identity Profile.

Configuring Authentication

If you select the Guest Registration option, the Guest Registration page appears as shown in Figure 5-14.

Figure 5-14. Guest Registration page



The screenshot shows a web browser window titled "Guest Registration - Microsoft Internet Explorer provided by America Online". The browser's address bar is empty. The main content area displays the HP logo (a blue circle with "hp" in white) and the word "invent" in a sans-serif font below it. A horizontal line separates the logo from a registration form. The form has a dark blue header with the text "Guest Registration" in white. Below the header, there are five input fields: "First Name:", "Last Name:", "Preferred Username:", "Password:", and "Password Confirmation:". Each field is a simple text box. At the bottom of the form is a "Register" button with a grey background and black text.

If you choose to require guests to register before logging on, the following process will occur when they log on to the system.

- The Guest user fills in their first and last name and selects a username and a password.
- The username and password are entered into the Rights Manager built-in database, and assigned to the Guest Identity Profile. Once registered, this user will be able to log in as a regular user (using the username and password he/she registered), but should still match the Guest Identity Profile and receive only Guest rights (as long as the Guest Identity Profile occurs in the Rights table prior to the default Authenticated Identity Profile).
- The user's first and last names are included in the entry created in the 700wl Series system log file 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.

Logoff Page Option

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. Go to the **Logon Page Text** section of the New/Edit Logon Customization page, as shown in Figure 5-12 on page 5-33.

Step 2. Place a check mark in the **Display logoff window after logging on** checkbox
Checking this option will cause a small logoff window to pop open when clients log on.

Note: This requires that the client browser be configured to use Javascript.

Step 3. Click **Save**.

Figure 5-15 shows the default Logoff page. If you have customized the logo for your Logon page, your logo replaces the HP logo on this page as well.

Figure 5-15. Logoff page



Customizing the Stop Page

When you change the logo in the **Logos** section of the Logon Customization page, the new logo also appears on the Stop page and the Logoff page.

If you want to change the text that appears on the Stop page, or the main Stop page image (the default is a stop sign) you can do that as well.

To change the text that appear on the Stop page:

Step 1. Go to the **Stop Page** section of the Logon Customization page (see Figure 5-12 on page 5-33).

Configuring Authentication

Step 2. In the textbox labeled **Stop Page Text** enter the text you want to display on the Stop page. This can include HTML formatting commands.

Step 3. Click **Save**.

To clear the stop page text after it has been set, click **Reset to Defaults** at the bottom of the page.

Note: Clicking **Reset to Defaults** will reset all the settings for this Logon Customization and Stop page to the default settings, not just the stop page text.

To change the main image on the Stop page (the default is a stop sign):

Step 1. In the **Stop Page Image** field, type the path and filename of a GIF, JPEG, PNG file, or other browser-compatible file format on your local system that contains the image you want to use, or click **Browse** to locate the proper directory and filename.

The filename of the current logo is displayed underneath the **Stop Page Image** field, along with the date that the logo was uploaded to the Rights Manager

Step 2. Click **Save**.

Figure 5-16. Stop page with custom logo, default text and Stop graphic



To restore the default Stop page graphic, click **Reset to Defaults** at the bottom of the page.

Note: Clicking **Reset to Defaults** will reset all the setting for this Logon Customization page to the default settings, not just the stop page image.

Customized Page Templates

If you want to create pages that are customized beyond the options provided on the Customize Web Pages by Connection Profile 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 C, “Creating Customized Templates” describes in detail how to create these templates.

Note: *The template files interact with the Logon Page settings on the Logon Customization 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 in the Logon Page section of the Logon Customization page. 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 that you have created based on the instructions in Appendix C, “Creating Customized Templates” do the following:

- Step 1.** From anywhere within the Rights Manager, click the **Log Customization** tab.
The Logon Customization page appears, showing the current list logon pages.
- Step 2.** Click **New Logon Customization...** or click on the name of an existing Logon Customization page.
The New, or Edit, Logon Customization page appears, depending on whether you clicked on **New Logon Customization...** or the name of an existing Logon Customization page.
- Step 3.** Click the Custom Templates tab at the top of the page. The page will display the Custom Templates information, see Figure 5-17.
The top part of the page, the **HTML Templates** section, contains the specification of the HTML templates to use for the logon page, the logoff page, the stop page, and the guest registration page. You can replace one or more of the standard page templates with your own template.

Note: *The templates you specify apply only to the named Logon Customization you are working with. If you wish to use multiple Logon Customizations, you need to specify any custom templates desired for each one.*

Configuring Authentication

Figure 5-17. Logon Customization: Custom Templates

The screenshot displays the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes the HP logo, the word "invent", and user information: "Username: admin", "Access Control Server: 192.168.10.116", and "Date & Time: Mon Feb 9 15:37:03 2004". Below the navigation bar are icons for STATUS, RIGHTS, NETWORK, VPN, MAINT, LOGS, HELP, and LOGOUT. The main navigation tabs are: Rights Setup, Identity Profiles, Connection Profiles, Authentication Policies, Access Policies, Logon Customization (selected), and Tools & Options.

The "New Logon Customization" page is shown. It has a "Name" field and a checkbox labeled "Make this the preferred Logon Customization for new Connection Profiles". The page is divided into two tabs: "Settings" and "Custom Templates" (selected). The "Custom Templates" tab contains instructions: "Provide the name of a customized template file in the appropriate field to replace a standard page template. If the custom page uses a custom image, provide the image file name in the Image File field. To delete a custom template, click the trash can button. Click Save to upload the specified files. See Help for further explanation."

The "HTML Templates" section lists the following fields, each with a "Browse..." button and a trash can icon:

- Logon Page
- Logoff Window
- Stop Page
- Guest Registration Page
- Logon Page Expired Page
- Logged Off Window
- Logoff Transition Page
- Too many Attempts Page

The "Template Images" section has a "New Image" field with a "Browse..." button and an "Upload Image" button.

At the bottom of the page are "Save", "Reset to Defaults", and "Cancel" buttons.

Step 4. In the appropriate field (**Logon Page**, **Logoff Window**, **Stop Page**, or **Guest Registration Page**), type the path and name of a `.tmpl` file on your local system that contains the template, or click **Browse** to locate the proper directory and file name.

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 5. In the **Custom Templates** tab of the New/Edit Logon Customization page, type the path and name of the image file (GIF, JPG, PNG, or other browser compatible file) located on your local system, in the **New Image** field or click **Browse** to locate the file.

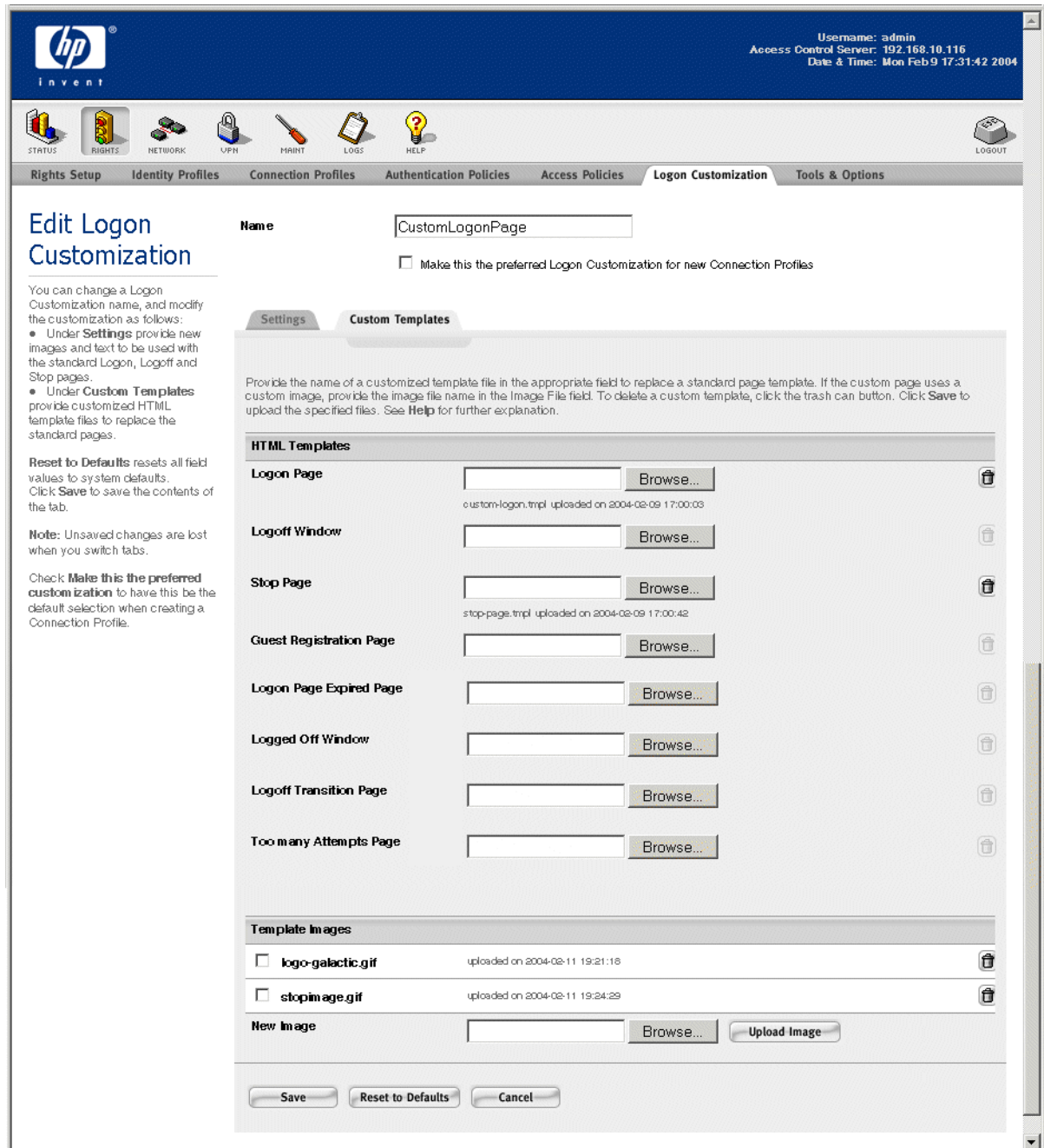
Step 6. Click **Upload Image** to add the graphic file to the Rights Manager.

The page will redisplay showing the loaded image, see Figure 5-18.

Note: The template images area shows ALL images available for use in custom templates, not just those you have loaded for a specific custom template.

To delete an image, click the trashcan icon on the same row at the graphic you wish to delete.

Figure 5-18. Custom Templates tab after images have been uploaded



Configuring Authentication

Step 7. To indicate that an image is to be used with the customized logon page you are creating, check the box to the left of the image. This notifies the system that this image should be downloaded to the Access Controller with the custom template code.

Note: Only those images you have checked will be sent to the Access Controller with the template code.

Step 8. Click **Save**.

The Administrative Console will return to the Logon Customization page.

Note: The HTML Template fields are 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, see Figure 5-18. If the default web page is in use, no message appears.

» To clear a template file and return to the default (built-in) page, click **Reset to Defaults**.

The default page is restored and the “Last Update at...” message is removed.

Note: Clicking **Reset to Defaults** will not delete any graphics you have loaded.

Tools and Options

The Tools and Options tab provides several options that help you manage and troubleshoot your Rights configuration. This area includes the following features:

- The User Rights Simulator — shows you the Connection Profile, Identity Profile, Access Policy, the logon expiration, and a detailed list of rights in XML format for a user you specify at a location and time you specify. You can use this to determine whether your Rights Assignment configuration is working as you expect, or to determine what rights a particular user would have if they logged on at a particular time through a particular Access Controller port.
- The Authentication Transaction Tracer — attempts to authenticate a user you specify using the Authentication Service you specify, and displays the information sent to and received from the service. You can use this to verify that an Authentication Service you have configured is working correctly.
- Import/Export Rights — lets you export the rights configuration and save it on an external system, or import a saved rights configuration from an external file. You can use this to copy a rights configuration from one Access Control Server to another. You can also use this as a method for modifying a rights configuration offline, by editing the saved configuration file.

Simulating User Rights

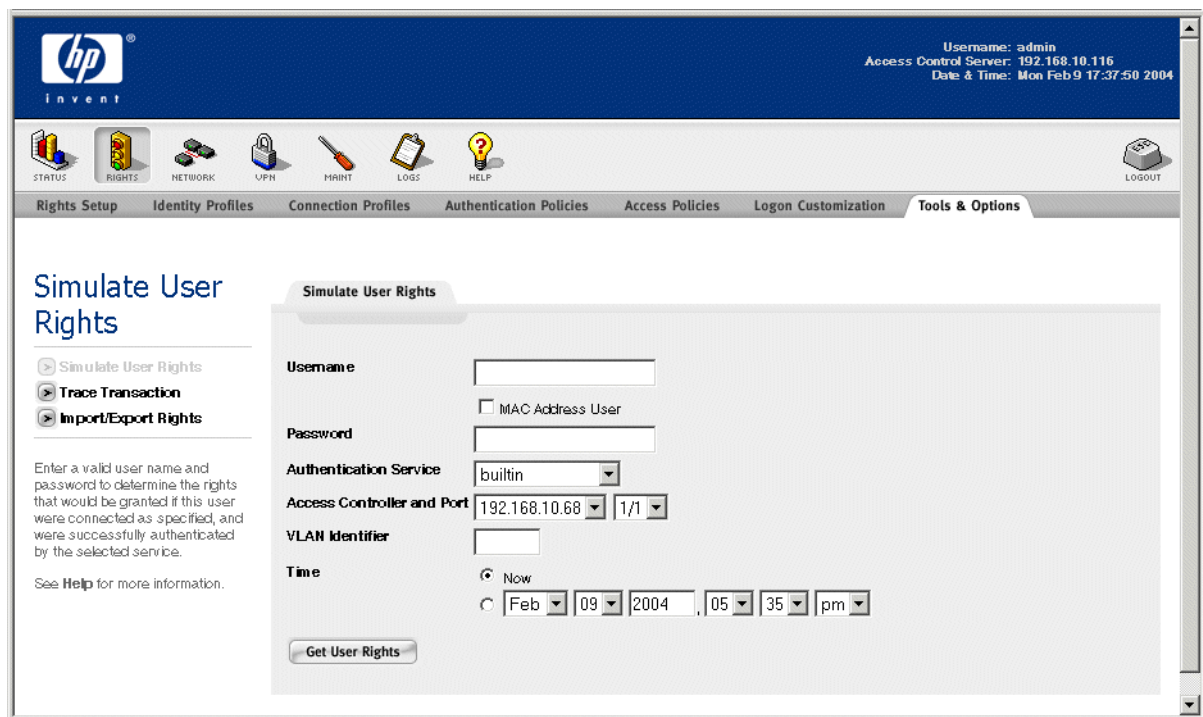
You can use the User Rights Simulator to view the rights that a particular user would receive if they were log on at a specific time and location. The 700wl Series system matches the user to an Identity Profile based on authentication via the Authentication Service you specify, and matches the use to a Connection Profile based on the Access Controller port, VLAN ID and connection time you specify. It then uses the Identity Profile and Connection Profile to determine the Access Policy appropriate for this user from the Rights Assignment table.

Note: 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 as if they were logged on at a particular time and location. To view the current rights for a logged-on user, see “Viewing Client Status” on page 3-7.

» To use the Rights Simulator, click the **Tools and Options** tab visible at the top of any Rights module page. This displays the Simulate User Rights page, as shown in Figure 5-19.

You can also access the User Rights Simulator from the Trace Transaction or Import/Export Rights pages by clicking the **Simulate User Rights** link in the left-hand column.

Figure 5-19. The Simulate User Rights Page



To simulate rights for a specific user, type information into the fields on this page as defined in Table 5-12:

Table 5-12. User Rights Simulator Fields

Field	Description
Username	The username (logon ID) of the user whose rights are to be simulated. Note: Guest users do not have logon IDs within the 700wl Series system, so in order to simulate Guest access rights you must use the logon ID of a “registered guest.” You can create a registered guest by adding a user to the built-in database and assigning it to the “Guest” identity profile.
MAC Address	Check this box if the “username” is really a MAC address.
Password	The password for this user.
Authentication Service	The Authentication Service to be used to authenticate this username. The results of the authentication is used to match the user to an Identity Profile/

Table 5-12. User Rights Simulator Fields

Field	Description
Access Controller and Port	The Access Controller, slot and port to be used to simulate the user's physical connection location. This is one of the elements used to match the user to a Connection Profile.
VLAN Identifier	The 802.1q VLAN tag normally included in packets from this user, if any. This is also one of the elements that may be used to match the user to a Connection Profile. If traffic from the user is untagged, leave this blank.
Time	The date and time of day to be use to simulate the time of the user's connection. This is also used in matching the user to a Connection Profile. Select Now if the current date and time should be used.

- » Click **Get User Rights** to submit the username for authentication, and retrieve their rights as specified. Figure 5-20 shows the rights for a Built-in user as if she were logged through slot 1/port 1 of the Integrated Access Manager, at the current time (Now), with no VLAN ID.

Figure 5-20. Rights for User “ann” if Logged on at the Specified Time and Location

The screenshot displays the HP ProCurve Rights Simulator interface. The top navigation bar includes links for STATUS, RIGHTS, NETWORK, UPN, HINT, LOGS, HELP, and LOGOUT. The main content area is titled "Simulate User Rights" and contains a form for inputting user details and a "Get User Rights" button. Below the form, the results are displayed in a table format, showing the Identity Profile, Connection Profile, Access Policy, and User Authentication Ends. At the bottom, the results are also shown in XML format.

Simulate User Rights

Username: ann
 MAC Address User
 Password:
 Authentication Service: builtin
 Access Controller and Port: 192.168.10.68 / 1/1
 VLAN Identifier:
 Time: Now Feb 09 2004 05 35 pm

User Rights for ann

Identity Profile	Authenticated
Connection Profile	Any
Access Policy	Authenticated
User Authentication Ends	Never

Rights in XML for ann

```
<?xml version="1.0" standalone="yes"?>
<client_rights mac="" id="ann" rights_id="2">
  <ip_addr_policy>do_nat</ip_addr_policy>
  <allow_static_ip>False</allow_static_ip>
  <encryption_required>False</encryption_required>
  <ipsec>
    <stance>Deny</stance>
  </ipsec>
  <pptp>
    <stance>Deny</stance>
    <mppe_bits>0</mppe_bits>
    <min_mschap>1</min_mschap>
    <allow_pap>False</allow_pap>
    <mppe_stateful>False</mppe_stateful>
  </pptp>
</client_rights>
```

The top portion of the Rights results shows the Identity Profile and Connection Profile that the user matched, based on the specified location, VLAN ID, and time, and the Access Policy that applies to this user as a result. It also shows when the user would be forced to reauthenticate.

- If the Connection Profile is not what you expected:
 - You may have entered the wrong slot and port, VLAN ID or time window into the Rights Simulator
 - The Connection Profile is defined differently than you expected
 - You may have multiple overlapping Connection Profiles, and this user is matching a Connection Profile in an earlier row in the Rights Assignment Table than you expected

Configuring Authentication

- If the Identity Profile is not what you expected:
 - For users in the built-in database, the user may have been assigned to a different profile than you expected.
 - If the user should match an Identity Profile based on a group or NT Domain name returned from an external authentication service, the service may be returning a different group name than you expected, or no matching Identity Profile has been created to match the group or Domain.
 - There may be multiple Identity Profiles that this user could match, and it is matching an Identity Profile in an earlier row in the Rights Assignment Table than you expected.
- If the Access Policy is not what you expected, you should review your Rights Assignment Table setup to determine whether you have multiple rows with the same Connection Profile and Identity Profile but different Access Policies. If this is the case, the user will always match on the first of these rows, and will never match on a later row. You should only have one row in the Rights Assignment Table for each unique combination of Connection Profiles and Identity Profiles.
- If the **User Authentication Ends** setting is not what you expect, check the **Timeout** setting in the Access Policy.

The bottom portion of the results shows the actual XML that defines the rights the user would receive (see Figure 5-21).

Figure 5-21. The XML Representation of User Rights

The screenshot shows a web browser window titled "HP ProCurve: Rights: Simulate User Rights - Microsoft Internet Explorer". The browser displays a configuration page with the following settings:

- Connection Profile: Any
- Access Policy: Authenticated
- User Authentication Ends: Never

Below these settings is a section titled "Rights in XML for ann" containing the following XML code:

```
<?xml version="1.0" standalone="yes"?>
<client_rights mac="" id="ann" rights_id="2">
  <ip_addr_policy>do_nat</ip_addr_policy>
  <allow_static_ip>False</allow_static_ip>
  <encryption_required>False</encryption_required>
  <ipsec>
    <stance>Deny</stance>
  </ipsec>
  <pptp>
    <stance>Deny</stance>
    <mppe_bits>0</mppe_bits>
    <min_mschap>1</min_mschap>
    <allow_pap>False</allow_pap>
    <mppe_stateful>False</mppe_stateful>
  </pptp>
  <l2tp>
    <stance>Deny</stance>
    <mppe_bits>0</mppe_bits>
    <min_mschap>1</min_mschap>
    <allow_pap>False</allow_pap>
    <mppe_stateful>False</mppe_stateful>
  </l2tp>
  <ssh>
    <stance>Deny</stance>
  </ssh>
  <up_allow_filters>
    <allow>ip</allow>
  </up_allow_filters>
  <up_ip_redirects>
    <ip_redirect>
      <match>tcp dst port 80 and dst host 1.1.1.1</match>
      <port>83</port>
      <ip>42.0.0.1</ip>
    </ip_redirect>
    <ip_redirect>
      <match>tcp dst port 443 and dst host 192.168.10.116</match>
      <port>443</port>
      <ip>42.0.0.1</ip>
    </ip_redirect>
  </up_ip_redirects>
  <expiry>800000</expiry>
  <reauth>-1</reauth>
  <logon_time>1076379498</logon_time>
  <location>
    <isNTuser>False</isNTuser>
    <locFlags>54</locFlags>
    <connName>Any</connName>
    <custName>Guest Reg page</custName>
  </location>
  <id>ann</id>
  <vlan_id>65535</vlan_id>
</client_rights>
```

Tracing Authentication Service Transactions

The Transaction Tracer lets you verify authentication transactions to one of the active authentication services—LDAP, RADIUS, Kerberos or XML-RPC. You can use this tool to verify that users are being authenticated correctly, and that the correct information is returned from the authentication service.

To use this tool, you select the authentication service you want to test, and enter the logon name and password of a user known to have a valid entry in the directory or service database. If the authentication

Configuring Authentication

service is working correctly, the service should return a successful result, including the information associated with that user, if appropriate. If the authentication service is not set up correctly, you will receive an error and incomplete results.

This tool cannot be used with the built-in database, and it cannot trace transactions based on the passive (or monitored) authentication services (802.1x and NT Domain logon)

Step 1. To use the Transaction Tracer, click the **Tools and Options** tab visible at the top of any Rights page. This displays the Simulate User Rights page.

Step 2. Click the **Trace Transaction** link in the left-hand column. The Transaction Tracer page appears, as shown in Figure 5-22.

Figure 5-22. The Trace Transaction page

Step 3. To trace the authentication transaction for a specific user, enter information into the fields on this page as shown in Table 5-13:

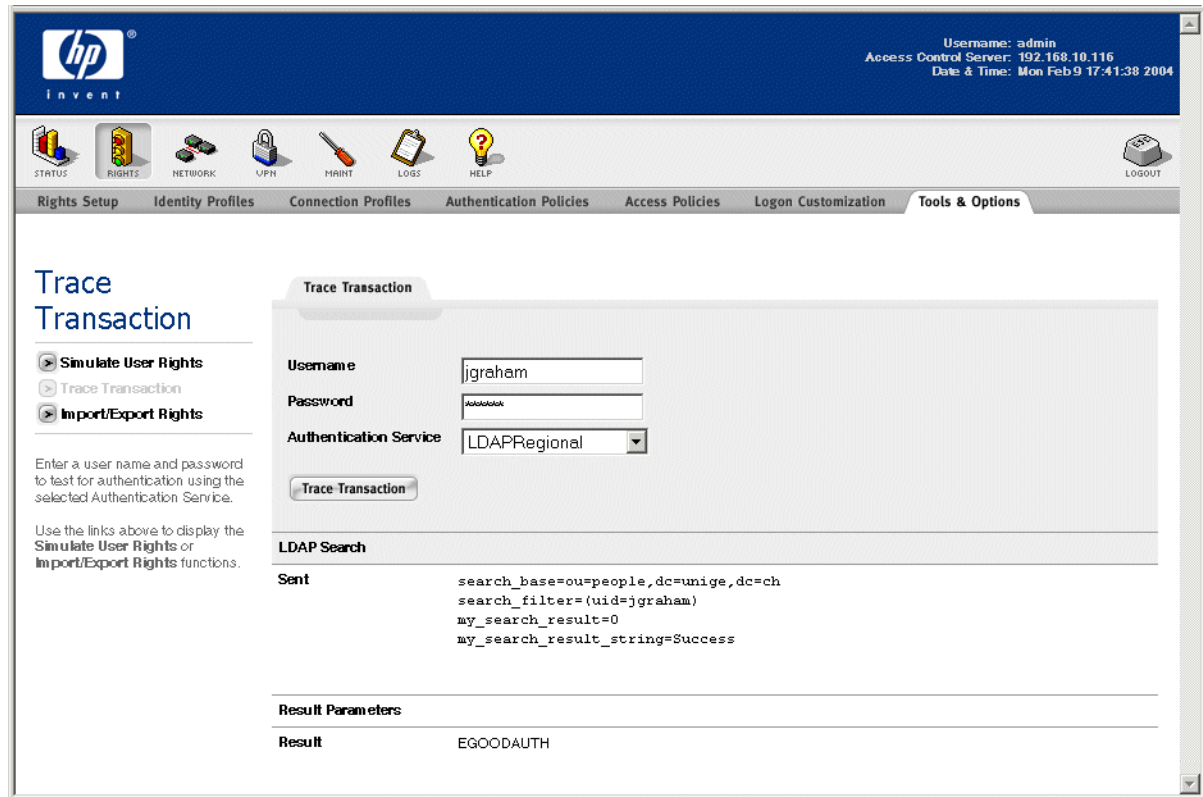
Table 5-13. Trace Authentication Transaction Fields

Field	Description
Username	The username (logon ID) of the user whose rights are to be simulated.
Password	The password for this user.
Authentication Service	The Authentication Service to be used to authenticate this username.

Step 4. Click **Trace Transaction** to submit the username for authentication. Figure 5-23 shows the authentication results for a user who was successfully authenticated against an LDAP database.

Note: When tracing a transaction to a RADIUS server, the Transaction Trace function uses PAP. Therefore in order to use the Transaction Trace function with RADIUS, you must enable PAP on your RADIUS server, even if you normally use MSCHAP.

Figure 5-23. Results of a traced transaction



The **Result Parameters** contain any parameters returned with the authentication, if appropriate. This will depend on the authentication service being used, and how that service has been configured (for example, whether you have it configured to return group information).

The **Result** displays a message indicating whether the authentication was successful or not.

Importing and Exporting the Rights Configuration

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.

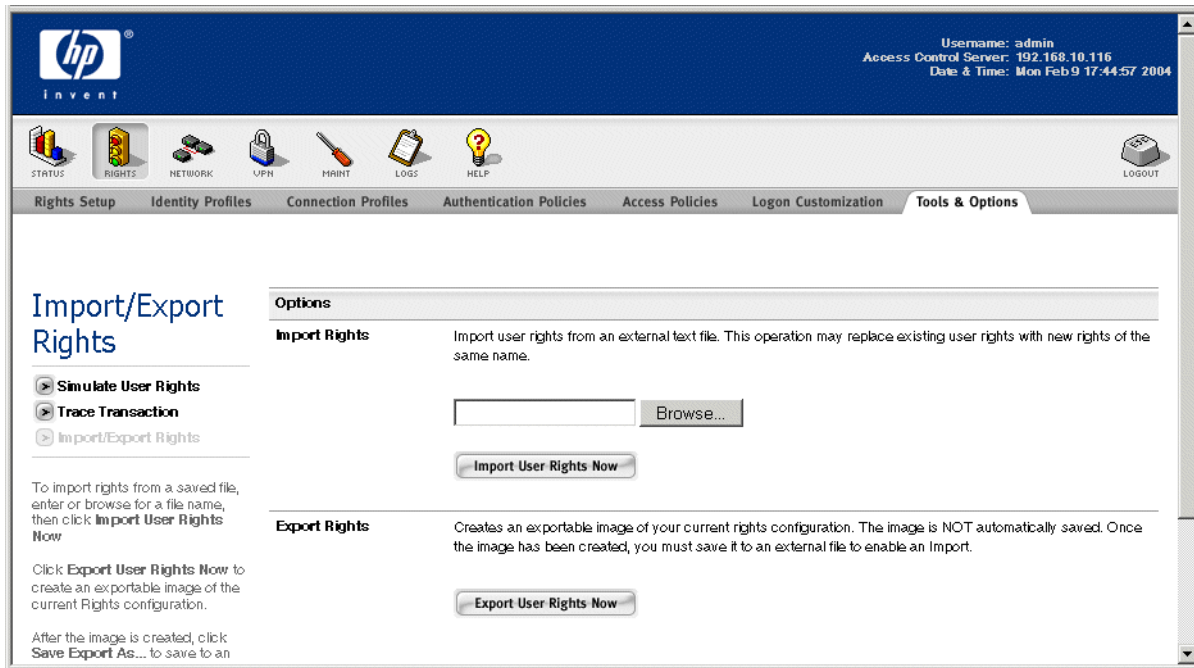
Note: *The import of rights is additive—the imported rights may replace rights of the same name in the target system, but any additional rights in the target system (that are not included in the imported set) will remain unchanged.*

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.

Configuring Authentication

- » To Import or Export Rights, click the **Tools and Options** tab visible at the top of any Rights module page, then click the **Import/Export Rights** link in the left-hand column of the page. This displays the Import/Export Rights page, as shown in Figure 5-24.

Figure 5-24. The Import/Export Rights page



Exporting Rights

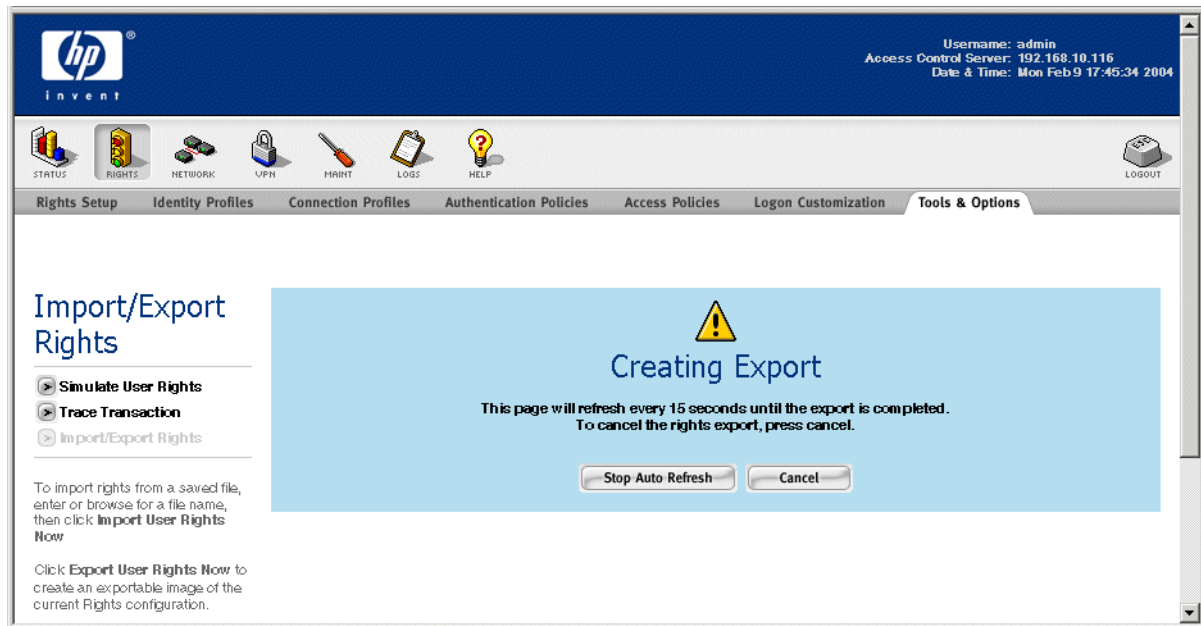
Exporting Rights is a two-step process — you must first create an exportable Rights image, then you can save the image to a file on an external system. If you subsequently do another Rights export, the new image will replace the previous one.

To create an exportable Rights image, do the following:

Step 1. Click **Export User Rights Now**.

The Import/Export Rights page changes to display an informational message to let you know the export has started (see Figure 5-25).

Figure 5-25. Rights Export in Progress page



While the export is in progress, this page is refreshed every 15 seconds.

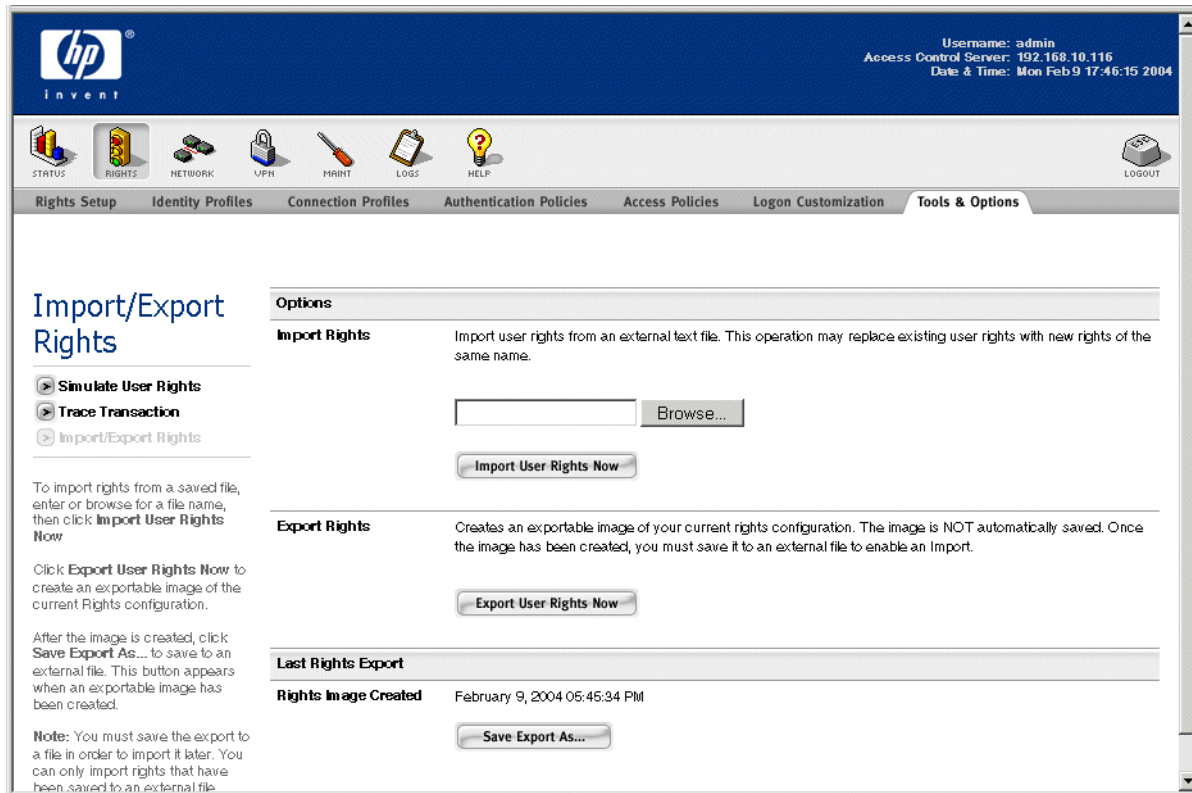
- To stop the page refresh, click **Stop Auto Refresh**.
- To cancel the import click **Cancel**.

Step 2. When the export has completed, another informational page appears, telling you the process is complete. This export image will replace the previous export image, if one existed.

- Click **Continue** to return to the main Import/Export Rights page.

When the export is done, a new field appears on the Import/Export Rights page, that indicates the date and time that the export was done, as shown in Figure 5-26.

Figure 5-26. The Import/Export Rights page after a successful rights export



Step 3. Under the **Last Rights Export** heading, click **Save Export As...** to save the rights export image as a file. This will start the file download process appropriate to your local system.

Step 4. 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.sql" but you can specify any name you want.

Importing Rights

When you import a saved set of rights, the 700wl Series system automatically creates a backup of the existing rights. If the import function fails (for example, if the import file is corrupted in some way) the system automatically restores the backed-up rights that it saved prior to doing the import.

To import a saved set of rights do the following:

Step 1. Type the name (including the path) of the file to be imported into the text box, or click **Browse...** to locate the file on your local system. By default an exported file is named `export.sql`.

Step 2. Click **Import User Rights Now** to begin the import process.

The Import/Export Rights page changes to display an informational message to let you know the import has started— this message initially indicates it is creating the rights backup.

While the import is in progress, this page is refreshed every 15 seconds.

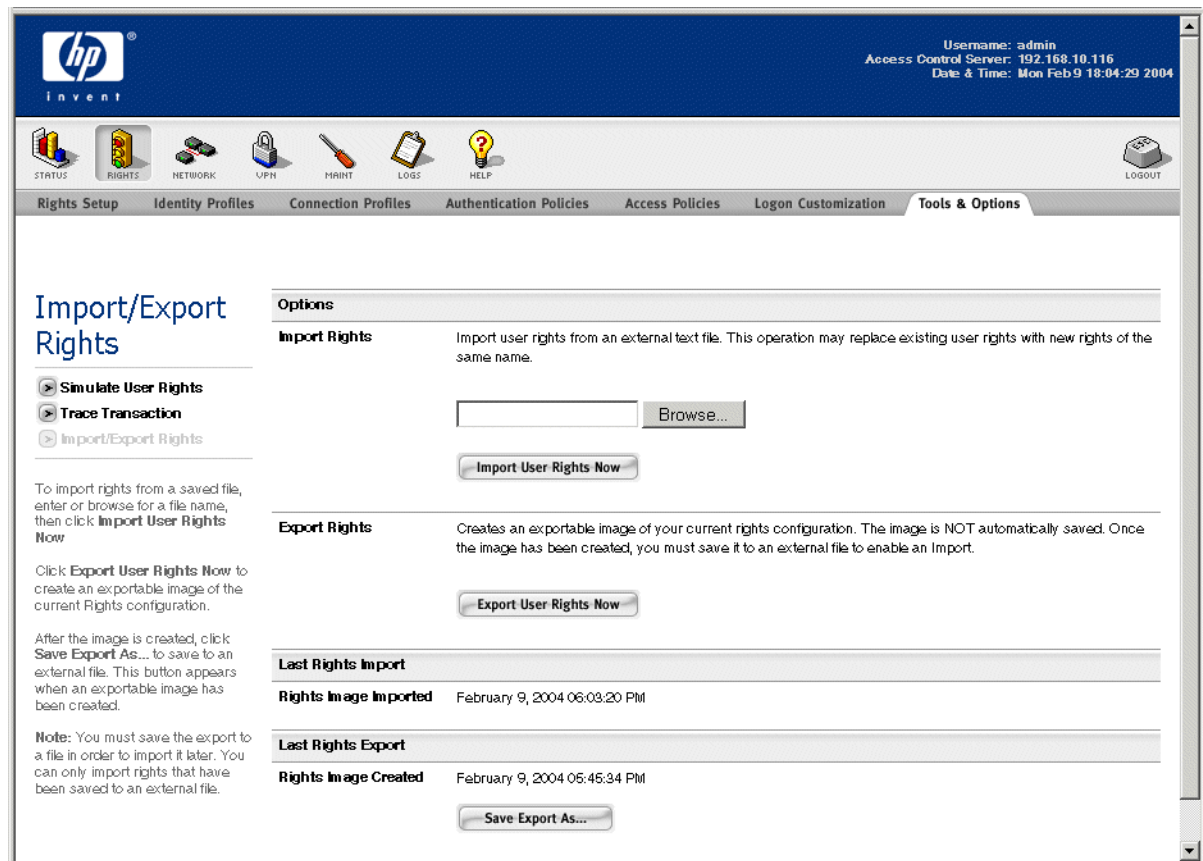
- To stop the page refresh, click **Stop Auto Refresh**.
- To cancel the import click **Cancel**.

Step 3. When the import has completed, another informational page appears, telling you the process is complete.

- Click **Continue** to return to the main Import/Export Rights page.

When the import is done, a new field appears on the Import/Export Rights page, that indicates the date and time that the import was done, as shown in Figure 5-27.

Figure 5-27. The Import/Export Rights page after a successful rights import



CONFIGURING THE NETWORK

This chapter describes how to configure the 700wl Series system components so that they work with your enterprise network. The topics covered in this chapter include:

700wl Series System Components	6-2
Configuring an Access Control Server	6-3
Configuring an Integrated Access Manager	6-7
Configuring Access Controllers	6-10
Configuring Failover with Redundant Access Control Servers	6-15
Configuring Network Communication—Network Setup	6-17
Configuring Network Interfaces	6-34
Configuring SNMP	6-38
Setting the Date and Time	6-40
Setting Up Administrators	6-42

Note: The functions described in this Chapter can be performed by a Super Administrator or Network Administrator. A Policy Administrator can only change his/her own administrator password (see “Editing Your Administrator Password” on page 6-45).

Note: A Network Administrator or Super Administrator can also use the 700wl Series system command-line interface (CLI) to configure the 700wl Series system. The CLI is described in Appendix A, “Command Line Interface”.

A 700wl Series system consists of an Access Control Server, that provides centralized administration for the system, and one or more Access Controllers, which monitor and control client connections and traffic to the network. A second Access Control Server may be used to provide automatic failover in a redundant configuration (see “Configuring Failover with Redundant Access Control Servers” on page 6-15 for more details).

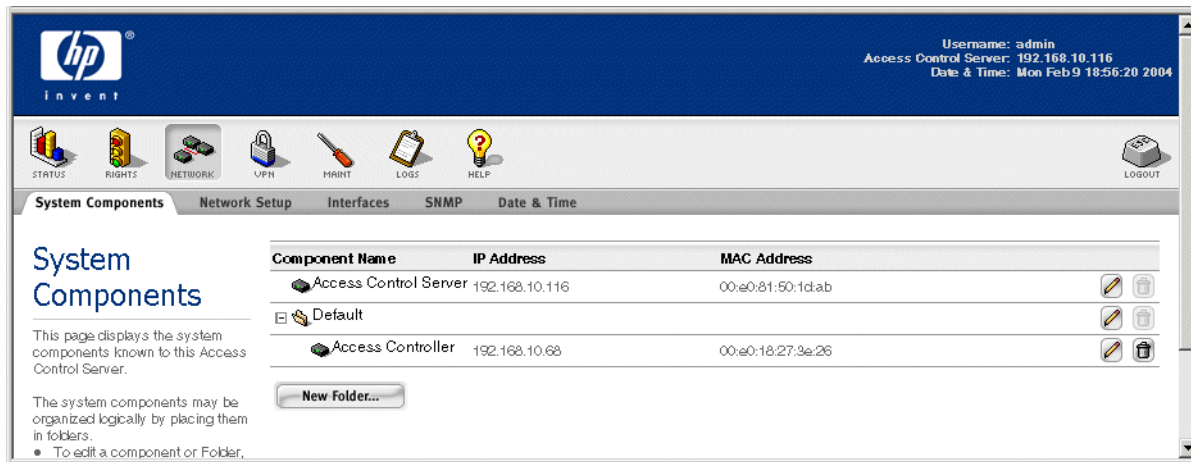
The configuration of the individual units that make up your 700wl Series system is done through the Network configuration pages, accessed by clicking the **Network** icon on the Navigation Toolbar. You can configure all the 700wl Series system components—Access Control Servers or an Integrated Access Manager and all Access Controllers—from one central location.

When you first click on the **Network** icon the system displays the contents of the System Components tab. Just below the navigation icons at the top of the page are a set of tab representing each of the main aspects of network configuration: System Components, Network Setup, Interfaces, SNMP, and Date & Time. Click the appropriate tab to reach the desired the network configuration page.

700wl Series System Components

When you first click on the **Network** icon the System Components page appears, as shown in Figure 6-1.

Figure 6-1. System Components Page



This page displays the System Components List, which lists all the 700wl Series system components known to the Access Control Server on which you are running the Administrative Console.

From the System Components tab you can:

- Modify the configuration of the Primary Access Control Server
- Add a secondary Access Control Server to the 700wl Series system for redundancy and failover
- Delete a Secondary Access Control Server (you cannot delete the Primary Access Control Server)
- Modify the Configuration of an Access Controller.

The System Components List

The System Components List shows the components of the 700wl Series system that are known to the Access Control Server. The list is in the form of a dynamic tree of components and *folders*. Folders are named groups of system components; they can be opened to show their contents or closed to simplify the display of the System Components List. (see “Organizing Access Controllers into Folders” on page 6-13).

The System Components List shows the following information:

Table 6-1. System Components List column definitions

Column	Description
Component Name	The alphanumeric name for the component, or the name of the Folder.
IP Address	The IP address of the Access Control Server, Access Controller, or Integrated Access Manager.
MAC address	The MAC address of the component.

From this list you can click a component name or click the pencil icon at the right of the row to edit the component's name and the folder to which it is assigned. For Access Control Servers, you can also edit settings related to its use in a failover configuration. See “Configuring an Access Control Server” on page 6-3 for more information.

You can delete some components using the trash can icon to the right. Some components cannot be deleted—in this case the trash can icon will be dimmed.

A more concise form of the System Components List, as shown in Figure 6-2 also appears on other pages under the Network, VPN, and Maintenance functions.

Figure 6-2. System Components List (Concise Version)



This list is also displayed in a tree form, with folders that can be opened or closed. The list enables you to select a component to view or modify as appropriate to the page you are viewing.

Configuring an Access Control Server

The Access Control Server provides centralized administration for the 700wl Series system. A second Access Control Server may be used to provide automatic failover in a redundant configuration (see “Configuring Failover with Redundant Access Control Servers” on page 6-15 for more details).

The Access Control Server on which you are running the Administrative Console already exists in the System Components List. In a redundant configuration, you can connect to the Administrative Console on either the primary or secondary Access Control Server.

The header bar of the Administrative Console indicates whether the Access Control Server you are logged into is the only Access Control Server in the system, or is the primary or secondary Access Control Server.

Editing the Access Control Server Configuration

The Access Control Server is typically configured with its network configuration parameters and shared secret when it is initially installed on the network, per the instructions in the *Quick Start Guide* or *Installation and Getting Started Guide* shipped with the hardware.

However, there are several situations in which you may need to modify the Access Control Server configuration:

- To function in a redundant configuration as either a Primary or Secondary Access Control Server
- To enable SSH access to the unit for remote CLI or Technical Support access
- To configure or change the shared secret used to establish a trust relationship between the Access Control Server and the associated Access Controllers, or with a peer Access Control Server in a redundant configuration.

Note: *The shared secret is normally configured on the Access Control Server at installation through the CLI. However, an Access Control Server configured to get its network parameters through*

Configuring the Network

DHCP (the default) will boot up and run properly without a shared secret configured, but Access Controllers will not be able to communicate with it. In this case, you must edit the Access Control Server configuration to add a shared secret to enable the Access Control Server to manage its associated Access Controllers. See “The Access Control Server Shared Secret” on page 6-7 for more information about the shared secret.

- » To edit an Access Control Server configuration, click on the name of the Access Control Server in the System Components List, or click the pencil icon (✎) to the far right of the Access Control Server.

The Edit Access Control Server page appears as shown in Figure 6-3.

Figure 6-3. Edit Access Control Server page

The screenshot shows the HP ProCurve management interface. At the top, there is a navigation bar with the HP logo and the word 'invent'. The user is logged in as 'admin' with the IP address '192.168.10.116' and the date/time 'Mon Feb 9 18:56:04 2004'. Below the navigation bar are several icons for 'STATUS', 'RIGHTS', 'NETWORK', 'UPN', 'MINT', 'LOGS', 'HELP', and 'LOGOUT'. The main content area is titled 'Edit Access Control Server' and contains the following fields and sections:

- Name:** Access Control Server
- IP Address:** 192.168.10.116
- MAC Address:** 00:e0:81:50:1d:ab
- Shared Secret:** [Redacted]
- Confirm Shared Secret:** [Redacted]
- Admin Username:** admin
- Admin Password:** [Redacted]
- Confirm Admin Password:** [Redacted]
- Enable HP ProCurve technical support access
- Enable SSH command line interface
- Redundancy:**
 - Preferred Primary Access Control Server
 - Enable Redundancy
 - A Peer IP Address has not been saved.
 - Peer Name:** [Redacted]
 - Peer IP Address:** [Redacted]
 - Failover Timeout:** 30 Seconds

At the bottom of the form are 'Save' and 'Cancel' buttons. On the left side of the form, there is instructional text and a list of bullet points:

- You can change the Access Control Server's name, shared secret, administrator and access permissions and redundancy configuration.
- To enable remote CLI access via SSH, check the box.
- Enable Technical Support Access *only* if requested to do so by your HP ProCurve technical support representative.
- To configure a redundant peer for this Access Control Server:
 - Specify a name and provide the IP address of the peer Access Control Server.
 - Specify a **Failover Timeout** (how long the peer Access Control Server waits to take control after losing contact with the primary).
 - Check **Preferred Primary Access Control Server** if this Access Control Server (not the peer) should be primary when redundancy is enabled.
 - Save the configuration.

You cannot enable redundancy until:

- a peer IP address is configured (and saved)
- that peer is reachable and responding
- one Access Control Server only is selected as Preferred Primary

To enable redundancy once the peer relationship is established, check **Enable Redundancy** and click **Save**. See **Help** for more information.

The fields on the Edit Access Control Server page show the current setting for the Access Control Server. You can modify any of these values, except the IP address and MAC Address, which are read-only fields.

Note: The IP address can be changed under the Network Setup tab, along with other network configuration settings.

The fields and options on this page are defined in Table 6-2:

Table 6-2. Edit Access Control Server page field definitions

Field/Option	Description
Name	An alphanumeric name for this Access Control Server. The default name is the IP address of the unit. A name may be up to 50 characters in length.
IP Address	The IP address of this Access Control Server (read-only). This can be changed under the Network Setup tab.
MAC address	The MAC address of this Access Control Server (read-only). This can be changed under the Network Setup tab.
Shared Secret	The shared secret used to establish a trust relationship between the Access Control Server and its Access Controllers. This must be set to a non-blank value. Note: Once a connection has been established between the Access Control Server and an Access Controller, changing the shared secret on the Access Control Server will not disrupt the connection. However, once the connection is lost, the Access Controller will not be able to re-establish the connection. Note: If this Access Control Server is in an active peer relationship (i.e. redundancy is enabled) you cannot change the shared secret. You must first disable redundancy.
Confirm Shared Secret	The shared secret, entered a second time to confirm.
Admin Username	The username for the built-in administrator of this Access Control Server. The default is <i>admin</i> . The name can be up to 50 characters.
Admin Password	The password for the built-in administrator of this Access Control Server. The default is <i>admin</i> . The password must be at least one (non-blank) character in length (a minimum of 5 is recommended).
Confirm Admin Password	The administrator password, entered a second time to confirm.
Enable HP ProCurve technical support access	(Optional.) A mark in this checkbox enables access by the Technical Support personnel at HP ProCurve to this Access Control Server. Note: Enable this feature only if directed to do so by your HP ProCurve Technical Support contact.
Enable SSH command line interface	(Optional.) A mark in this checkbox enables remote access to the Command Line Interface for this Access Control Server via SSH. This requires that the client system running the CLI supports SSH. If this checkbox is not checked, remote access to the CLI is disabled, and the CLI can be accessed only over a direct connection to the serial port on the Access Control Server. This option is enabled by default.

Table 6-2. Edit Access Control Server page field definitions

Field/Option	Description
Redundancy	
Preferred Primary Access Control Server	<p>If checked, specifies that this Access Control Server (the one on which this configuration is being done, not the peer Access Control Server) should be the primary Access Control Server upon enabling redundancy.</p> <p>One (and only one) peer must have this option checked.</p> <p>Do not check this option if this Access Control Server is intended to function initially as a secondary Access Control Server.</p> <p>Note: <i>If this Access Control Server is in an active peer relationship (i.e. redundancy is enabled) you cannot change the preferred primary designation. You must first disable redundancy.</i></p>
Enable Redundancy	<p>Check to enable the Access Control Server redundancy/failover feature, and begin the data synchronization process.</p> <ul style="list-style-type: none"> • A peer Access Control Server must be configured (i.e. the IP address entered and saved). • The peer Access Control Server must be reachable and responding • One Access Control Server must have the Preferred Primary option checked. <p>The Enable Redundancy checkbox is not selectable if these conditions are not met. A message below the checkbox indicates the reason it is not selectable.</p> <p>Warning: <i>The data synchronization process will overwrite most of the configuration on the secondary Access Control Server.</i></p>
Peer Name	<p>An alphanumeric name for the peer Access Control Server. The name may be up to 50 characters in length.</p>
IP Address	<p>The IP address of the peer Access Control Server.</p> <p>Note: <i>If this Access Control Server is in an active peer relationship (i.e. redundancy is enabled) you cannot change the IP address of the redundant peer. You must first disable redundancy.</i></p>
Failover Timeout	<p>The time interval, in seconds, used by the peer Access Control Server to determine that the primary Access Control Server is no longer operational. The Secondary Access Control Server will take over at that point. See “Configuring Failover with Redundant Access Control Servers” on page 6-15 for more information on failover latency.</p> <p>Note: <i>If this Access Control Server is in an active peer relationship (i.e. redundancy is enabled) you cannot change the failover timeout. You must first disable redundancy.</i></p>

- » To modify the Access Control Server settings, edit the desired fields and click **Save**.
 To abandon your changes and revert to the current settings click **Cancel**.

Deleting a Peer Access Control Server

You must disable redundancy by editing the Primary Access Control Server configuration before you can delete the Secondary Access Control Server (uncheck the Enable Redundancy checkbox and **Save**).

To delete a peer Access Control Server once redundancy is disabled, click the trash can icon () to the far right of the Access Control Server in the System Components List.

You can also delete a peer Access Control Server, by changing the Peer IP address to 0.0.0.0.

Note: *You cannot delete the Access Control Server on which you are running, and you cannot delete the peer Access Control Server while redundancy is enabled.*

The Access Control Server Shared Secret

Each Access Controller system must prove to its Access Control Server (or Integrated Access Manager) that it is trustworthy. A *shared secret*, initially established on the Access Control Server, is used between the Access Controller and the Access Control Server to establish this trust relationship. (The exception is that a shared secret is not necessary for communication between the internal Access Controller and the Access Control Server function of an Integrated Access Manager.)

In order for an Access Controller to communicate with an Access Control Server, it must be configured with the Access Control Server's IP address and the correct shared secret. The Access Control Server must be configured with its IP address (or receive it via DHCP) and the shared secret must be determined before an Access Controller can be configured to communicate with it. Each Access Controller that will be connected to the Access Control Server must then be configured with the Access Control Server's IP address and a matching shared secret.

The *Quick Start Guide* and the *Installation and Getting Started Guide* for your hardware both include setting the shared secret as part of the initial hardware installation on the network. This is done using the Command Line Interface (CLI) over the serial port. The *Access Controller Quick Start Guide* leads you through entering these commands on your Access Controller.

Once the Access Controller can communicate with the Access Control Server, shared secret changes will be propagated from the Access Control Server to the Access Controller as long as the Access Controller is connected at the time the shared secret is changed. If the shared secret is changed while an Access Controller is disconnected or otherwise cannot communicate with the Access Control Server, the new shared secret will need to be entered using the CLI.

Configuring an Integrated Access Manager

An Integrated Access Manager combines an Access Control Server and an Access Controller in a single chassis. Thus, an Integrated Access Manager can be used to provide centralized administration for the 700wl Series system in the same way as an Access Control Server does.

Note: *An Integrated Access Manager cannot be configured as a peer in a redundancy configuration.*


Editing the Integrated Access Manager Configuration

The Integrated Access Manager is typically configured with its network configuration parameters and shared secret when it is initially installed on the network, per the instructions in the *Quick Start Guide* or *Installation and Getting Started Guide* shipped with the hardware.

However, there are several situations in which you may need to modify the Integrated Access Manager configuration:

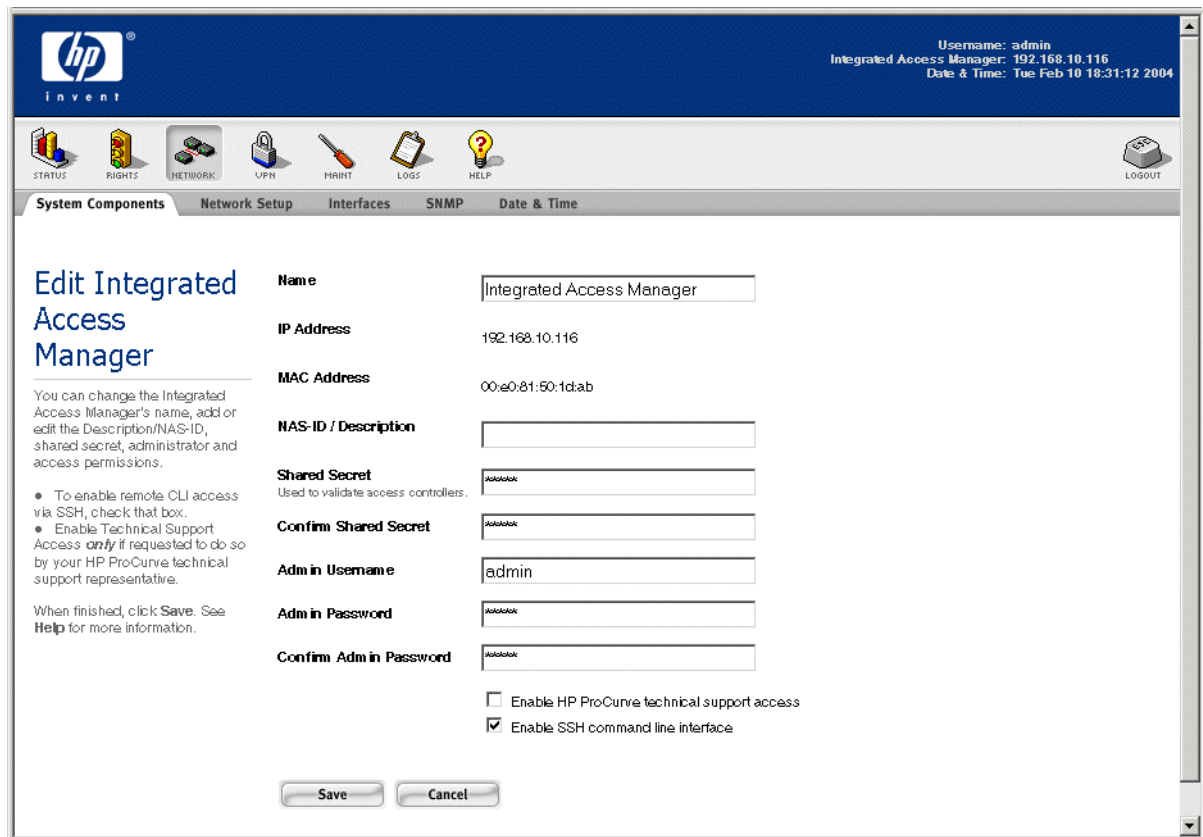
- To enable SSH access to the unit for remote CLI or Technical Support access
- To configure or change the shared secret used to establish a trust relationship between the Integrated Access Manager and the associated Access Controllers.

Note: *The shared secret is normally configured on the Integrated Access Manager at installation through the CLI. However, an Integrated Access Manager configured to get its network parameters through DHCP (the default) will boot up and run properly without a shared secret configured, but separate Access Controllers will not be able to communicate with it. In this case, you must edit the Integrated Access Manager configuration to add a shared secret to enable the Integrated Access Manager to manage its associated Access Controllers. See “The Access Control Server Shared Secret” on page 6-7 for more information about the shared secret.*

- » To edit a Integrated Access Manager configuration, click on the name of the Integrated Access Manager in the System Components List, or click the pencil icon () to the far right of the Integrated Access Manager.

The Edit Integrated Access Manager page appears as shown in Figure 6-4.

Figure 6-4. Edit Integrated Access Manager page



The fields on the Edit Integrated Access Manager page show the current setting for the Integrated Access Manager. You can modify any of these values, except the IP address and MAC Address, which are read-only fields.

Note: The IP address can be changed under the Network Setup tab, along with other network configuration settings.

The fields and options on this page are defined in Table 6-3:

Table 6-3. Edit Integrated Access Manager page field definitions

Field/Option	Description
Name	An alphanumeric name for this Integrated Access Manager. The default name is the IP address of the unit. Names can be up to 50 characters in length.
IP Address	The IP address of this Integrated Access Manager (read-only). This can be changed under the Network Setup tab.
MAC address	The MAC address of this Integrated Access Manager (read-only). This can be changed under the Network Setup tab.

Table 6-3. Edit Integrated Access Manager page field definitions

Field/Option	Description
NAS-ID/Description	A description for this unit. If using RADIUS accounting, this field is used as the NAS-ID and is sent to the RADIUS server as part of the accounting information. (If you do not enter a NAS-ID, the MAC address of the Integrated Access Manager is sent instead.) See “Using RADIUS for Accounting” on page 5-20 for more details about the RADIUS accounting feature.
Shared Secret	The shared secret used to establish a trust relationship between the Integrated Access Manager and any separate Access Controllers (the shared secret does not affect the internal Access Controller). Note: <i>Once a connection has been established between the Integrated Access Manager and an external Access Controller, changing the shared secret on the Integrated Access Manager will not disrupt the connection. However, once the connection is lost, the Access Controller will not be able to re-establish the connection. IP address) in order to communicate with the Access Control Server.</i>
Confirm Shared Secret	The shared secret, entered a second time to confirm.
Admin Username	The username for the built-in administrator of this Integrated Access Manager. The default is <i>admin</i> . The name can be up to 50 characters.
Admin Password	The password for the built-in administrator of this Integrated Access Manager. The default is <i>admin</i> . The password must be at least one (non-blank) character in length (a minimum of 5 is recommended).
Confirm Admin Password	The administrator password, entered a second time to confirm.
Enable HP ProCurve technical support access	(Optional.) A mark in this checkbox enables access by the Technical Support personnel at HP ProCurve to this Access Control Server. Note: <i>Enable this feature only if directed to do so by your HP ProCurve Technical Support contact.</i>
Enable SSH command line interface	(Optional.) A mark in this checkbox enables remote access to the Command Line Interface for this Integrated Access Manager via SSH. This requires that the client system running the CLI supports SSH. If this checkbox is not checked, remote access to the CLI is disabled. The CLI can be accessed only over a direct connection to the serial port on the Integrated Access Manager.

- » To modify the Integrated Access Manager settings, edit the desired fields and click **Save**.
To abandon your changes and revert to the current settings click **Cancel**.

Configuring Access Controllers

An Access Controller that has been installed on the network and configured to communicate with the Access Control Server (with the Access Control Server’s IP address and shared secret) appears automatically in the System Components List.

With the exception of the Access Control Server IP address and shared secret, Access Controllers are configured centrally from the Administrative Interface of the Access Control Server or Integrated Access Manager. From the Administrative Console you can configure and delete Access Controllers, as well as organize them into folders.

Note: Once the Access Control Server has recognized and is managing an Access Controller, you should not attempt to configure the Access Controller directly through the CLI, as doing so may conflict with the settings maintained for the Access Controller by the Access Control Server.

- » To edit an Access Controller's settings, click the name of the Access Controller in the System Components List, or click the pencil icon (✎) to the far right. If the Access Controller is in a folder that is closed, you will need to open the folder before you can select the Access Controller.

The Edit Access Controller page appears. See Figure 6-5.

Figure 6-5. Edit Access Controller Page

The screenshot shows the 'Edit Access Controller' page in the HP ProCurve Administrative Interface. The page header includes the HP logo and the text 'invent'. The top right corner displays the user's login information: 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Wed Mar 3 15:31:16 2004'. Below the header is a navigation bar with tabs for 'System Components', 'Network Setup', 'Interfaces', 'SNMP', 'Date & Time', and 'Admin Setup'. The main content area is titled 'Edit Access Controller' and contains a description of the page's purpose. Below the description are several form fields for editing the controller's settings, including Name, IP Address, MAC Address, NAS-ID / Description, Admin Username, Admin Password, Confirm Admin Password, Folder, and Access Control Server settings (Control Server IP, Shared Secret, Confirm Shared Secret). There are also checkboxes for 'Enable HP ProCurve technical support access' and 'Enable SSH command line interface'. At the bottom, there are 'Save' and 'Cancel' buttons.

The fields on the Edit Access Controller page show the current setting for the Access Controller. This includes the following information:

Table 6-4. Edit Access Controller page fields

Field/Checkbox	Description
Name	An alphanumeric name for the Access Controller. By default the name is the IP address of the unit.
IP Address	The IP address of this Access Controller (read-only). This can be changed under the Network Setup tab.
MAC address	The MAC address of this Access Controller (read-only). This can be changed under the Network Setup tab.
NAS-ID/Description	A description for this Access Controller. If using RADIUS accounting, this is used as the NAS-ID and is sent to the RADIUS server as part of the accounting information. (If you do not enter a NAS-ID, the MAC address of the Access Controller is sent instead.) See “Using RADIUS for Accounting” on page 5-20 for more details about the RADIUS accounting feature.
Admin Username	The built-in administrator username for this Access Controller. The default is <i>admin</i> . The name can be up to 50 characters.
Admin Password	The built-in administrator password for this Access Controller. The default is <i>admin</i> . The password must be at least one (non-blank) character in length (a minimum of 5 is recommended).
Confirm Admin Password	The administrator password, entered a second time to confirm.
Folder	(Optional.) The name of the folder in which to place this Access Controller. Pull down the list to select a folder. By default the Access Controller is placed in the Default folder. See “Folders vs. Locations” on page 6-14 for more information on Folders.
Enable HP ProCurve technical support access	(Optional.) A check in this checkbox enables access by the Technical Support personnel at HP ProCurve to this Access Controller. Note: Enable this feature only if directed to do so by your HP ProCurve Technical Support contact.
Enable SSH command line interface	(Optional.) A check in this checkbox enables remote access to the Command Line Interface for this Access Controller via SSH. This requires that the client system running the CLI supports SSH. If this checkbox is not checked, remote access to the CLI is disabled. The CLI can be accessed only over a direct connection to the serial port on the Access Controller.
Access Control Server	
Access Control Server IP	The IP address of the Access Control Server (or Integrated Access Manager) to which this Access Controller should be connected.
Shared Secret	The shared secret used to validate this Access Controller to its Access Control Server or Integrated Access Manager. It must match exactly the shared secret configured on the Access Control Server or Integrated Access Manager.
Confirm Shared Secret	The shared secret, entered a second time to confirm.

You can modify an Access Controller's name, administrator username and password, folder, SSH access permissions, and the Access Control Server IP address and shared secret. The IP address and MAC address are displayed read-only and cannot be modified on this page.

- » Click **Save** to save your changes, or **Cancel** to abandon your changes and revert to the current settings.

Note: *The IP address of the Access Controller can be changed under the Network Setup tab, along with other network configuration settings.*

Deleting an Access Controller

Access Controllers that have been removed from the network or reconfigured to communicate with a different Access Control Server are *not* automatically deleted from the Access Control Server's list of Access Controllers. They remain in the list on the assumption that the inability to communicate is temporary, and that the configurations should be maintained in the event that communication is reestablished. If you know that an Access Controller has been permanently removed from this Access Control Server's administrative domain, you must delete the Access Controller from the System Components List. Otherwise the Access Control Server will attempt to contact the removed Access Controller for status updates and wait for the Access Controller to respond.

- » To delete an Access Controller from the System Components List, click the trash can icon () at the far right of the Access Controller in the System Components List.

You cannot delete an Access Controller if it is in use—i.e. if it is used in the definition of a Location. Before you can delete an Access Controller, you must remove it from any Location definitions. If the Access Controller is the only component used in a Location definition, that Location must be redefined or deleted. In turn, you will not be able to delete the Location if it is used to define a Connection Profile.

Note: *If the Access Controller you delete is still connected to the network, and is still configured with the Access Control Server IP address and shared secret, it will not remain deleted. It will reappear as if it were a newly-installed Access Controller the next time it communicates with this Access Control Server. Any configuration you had done to that Access Controller through the Administrative Console will be cleared.*

Organizing Access Controllers into Folders

Folders allow the grouping of Access Controllers within the System Components List. For example, all the Access Controllers in a building could be placed in a single folder named after the building, such as *Building A*. You may create folders as needed. Within the System Components List, folders can be opened to show all their contents or closed to allow a high-level view of the system.

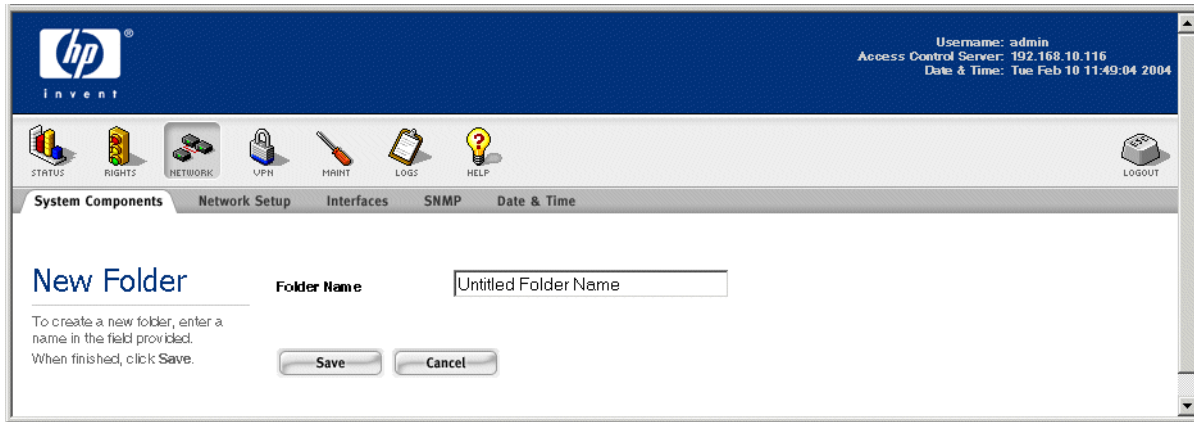
- » To create a new folder, click the **New Folder ...** button at the bottom of the page. This displays the New Folder page, see Figure 6-6. Enter the name for the folder and click **Save**.

To abandon your changes and revert to the current settings click **Cancel**.

Note: *Folders cannot be nested.*

Folders and the Access Controllers within them are listed in alphabetical order.

Figure 6-6. New Folder Page



- » To change the name of a folder, click the folder name in the System Components List, or click the pencil icon (✎) to the far right of the folder. Either action displays the Edit Folder page. Enter the new folder name in the **Folder Name** field and click **Save**.
- » To add an Access Controller to a folder, go to the Edit Access Controller page and select the folder by name from the drop-down **Folder** list, then click **Save**. See “Configuring Access Controllers” on page 6-10.
- » To remove an Access Controller from a folder, go to the Edit Access Controller page and either select a different folder from the drop-down **Folder** list in which to place the Access Controller, or select “None” from the drop-down **Folder** list, then click **Save**. See “Configuring Access Controllers” on page 6-10.
- » To delete a folder, click the trash can icon (🗑) to the far right of the folder in the System Components List.

Note: You cannot delete a folder that has Access Controllers in it—the trash can icon will be dimmed and not selectable.

Folders vs. Locations

The 700wl Series system provides two means of grouping its physical components: Folders and Locations.

- *Folders* are used within the Administrative Console as a way to organize Access Controllers in the System Components List for convenience in the configuration, management, and monitoring of system components.
- *Locations* are used within the Rights Management system to logically group sets of Access Controller ports to define the physical locations through which clients may connect to the 700wl Series system. The client’s physical location is one of the factors that determines the access rights eventually granted to that client. See Chapter 4, “Configuring Rights” for a much more detailed explanation of Locations and how they are used within the Rights Management system.

A Location may consist of selected ports from multiple Access Controllers—the grouping is based on sets of ports that should be associated with a common Access Policy (or set of access rights).

Configuring Failover with Redundant Access Control Servers

Please read the section “Enterprise Class Redundancy” on page 2-18 in Chapter 2, “Configuring the Network”

Note: *Integrated Access Managers cannot be used as a peer in a redundant configuration.*

The 700wl Series system supports multiple Access Control Servers for Access Control Server redundancy and failover. Access Control Server failover provides high availability operation for clients in case of system outages, network failures, etc. The primary Access Control Server functions as a normal Access Control Server, servicing the connected Access Controllers requests for authentication, rights administration, and other functions. The redundant Access Control Server is synchronized with the primary Access Control Server through a combination of database replication, message/state replication, and configuration replication, and is kept synchronized via incremental SQL updates.

To set up a redundant Access Control Server configuration, the following is required:

- Two peer Access Control Servers, each running version 4.0 or later software, must exist on the network, and be mutually reachable.
- One of these Access Control Servers must have the **Preferred Primary Access Control Server** option checked as part of the Access Control Server setup under the System Components tab of the Network pages. *Only one of the peer Access Control Servers may have this option checked.*
- Both Access Control Servers (and all Access Controllers) must be configured with the same shared secret in order to communicate with each other and with the Access Controllers under their control.
- As Access Controllers are installed on the network, they should be configured with the IP address of the Preferred Primary Access Control Server. Access Controllers in a configuration with redundant Access Control Servers receive the address of the peer Access Control Server from the Primary Access Control Server.

The process of configuring a 700wl Series system to use redundant Access Control Servers is as follows:

- Step 1.** Select one of the two Access Control Servers to function as the Preferred Primary Access Control Server. This Access Control Server will be the one that initially manages the Access Controllers associated with the 700wl Series system, and will be the one responsible for initiating the redundant peer relationship with its peer Access Control Server. In addition, in case of a simultaneous reboot of both peer Access Control Servers, the one designated the Preferred Primary will take control of the associated Access Controllers.
- Step 2.** Prepare a second Access Control Server to function as a redundant peer by configuring its shared secret to be the same as the primary Access Control Server’s shared secret. The second peer Access Control Server must *not* be designated as the Preferred Primary Access Control Server. This Access Control Server does not need to be configured beyond the basic network configuration settings—once the process of synchronization with its peer begins, most configuration information on the secondary Access Control Server will be overwritten by the configuration from the primary Access Control Server.
- Step 3.** On the primary Access Control Server, provide a name, for the peer Access Control Server, enter the IP address of the second Access Control Server as the Peer IP Address, check the **Preferred Primary Access Control Server** setting, and **Save** these changes.

Note: *You cannot enable redundancy (the check box will not be active) until a connection with the peer Access Control Server has been established.*

Configuring the Network

Step 4. When you are ready to initiate the peer relationship and start the data synchronization process, check the **Enable Redundancy** checkbox on the Primary Access Control Server (and **Save**). You only need to configure and enable redundancy on the primary Access Control Server to make the relationship active.

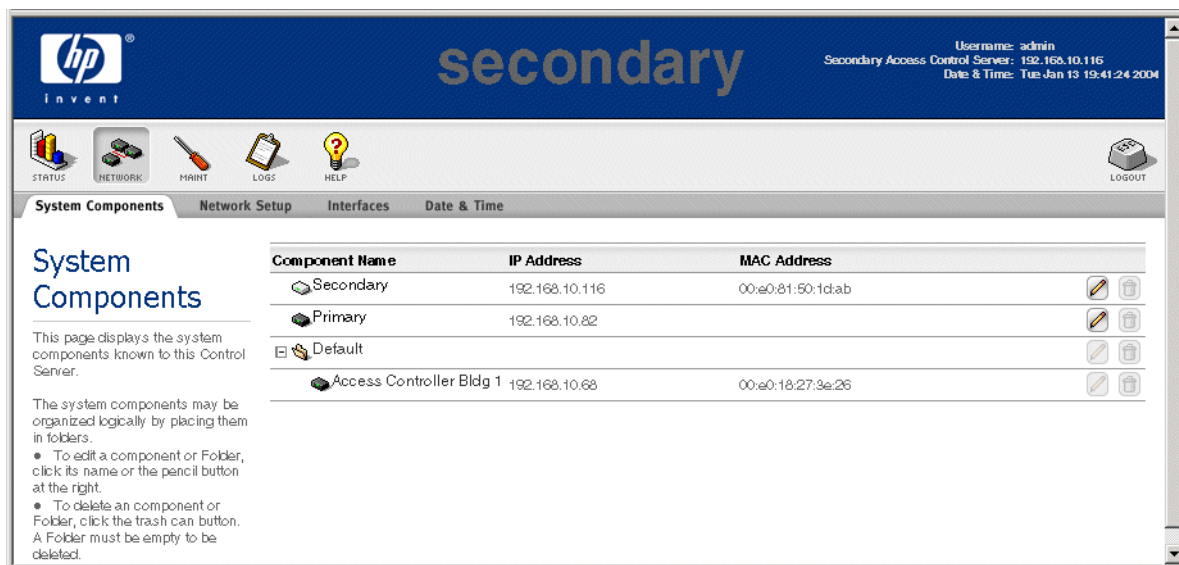
Note: *Once the redundant peer relationship is active, the configuration on the secondary Access Control Server is overwritten by the configuration of the primary Access Control Server. It is recommended that you back up the second Access Control Server before you initiate the peer relationship.*

Once redundancy is operational, refreshing the browser window changes the Access Control Server label at the upper right of the Header bar to indicate whether the Access Control Server is acting as a primary or secondary Access Control Server.

When running the Administrative Console on the primary Access Control Server, the label in the Header bar will show “Primary Access Control Server”.

When running the Administrative Console on the secondary Access Control Server, the Header bar label shows “Secondary Access Control Server”, and the word “secondary” appears in large letters in the center of the Header bar, as shown in Figure 6-7.

Figure 6-7. System Components list of a Secondary Access Control Server



The Secondary Access Control Server

A secondary Access Control Server does not support a full set of configuration capabilities. Only minimal network configuration and maintenance functions (such as software update, backup and restore) are allowed. The Rights and VPN functions are not available at all from a secondary Access Control Server Administrative Console. Within the remaining functions, the following capabilities are supported:

- Under **Status**, the Equipment Status tab is available, but you cannot view Client Status or Session Status.

- Under **Network**, only the System Components, Network Setup, Interfaces, and Date & Time tabs are available.
- Under **Maintenance**, and **Logs**, all the functions are available.

Disabling Redundancy

When you disable redundancy, the secondary Access Control Server is reset to Factory Defaults and restarted. This is necessary to prevent that Access Control Server from retaining knowledge of the Access Controllers—otherwise it is possible that it could take management control of the Access Controllers away from the primary Access Control Server.

Because the secondary Access Control Server is reset to its defaults, if you want to then re-establish a redundant peer relationship, you must reconfigure the secondary Access Control Server with the Preferred Primary Access Control Server shared secret. In addition, if the Factory Reset on the secondary Access Control Server caused the IP address of the Access Control Server to change, you may need to reconfigure the Peer IP address in the Preferred Primary Access Control Server's redundancy configuration.

To disable redundancy:

- » From the Edit Access Control Server page on the Access Control Server where you configured and enabled redundancy (normally the Preferred Primary Access Control Server), uncheck the **Enable Redundancy** checkbox, then click **Save**.

This stops the redundancy relationship, and *causes a restart with Factory Reset on the secondary Access Control Server*. At this point the primary Access Control Server still retains its knowledge of the peer Access Control Server's IP address; however, if the Factory Reset on the peer causes its IP address to change, the primary Access Control Server will show the secondary as "Not Responding" on the Equipment Status page.

To completely dismantle the redundant peer configuration, so that the primary Access Control Server no longer shows a peer Access Control Server, do the following:

- » On the System Components page, the trash can icon should now be enabled for the peer (second) Access Control Server. Click the trash can to remove the Secondary Access Control Server.

This removes the peer Access Control Server from the System Components List, and the fields in the Redundancy area of the Edit Access Control Server tab should be cleared. The Access Control Server label in the Header bar should now show just "Access Control Server."

You can also effectively delete the peer Access Control Server from the primary's System Components List by changing the Peer IP Address to 0.0.0.0.

Configuring Network Communication—Network Setup

Once the system components have been established, they must be configured to communicate with the network. The *Installation and Getting Started Guide* for your 700w1 Series system leads you through the initial network configuration sufficient for installation on your network. However, if your network configuration changes after installation, you can modify the settings for your system components through the Administrative Interface. In addition, there are advanced settings and other configuration options you may need to set up after the initial installation.

Configuring the Network

- » To access the Network Setup pages, click the **Network** icon in the Navigation Toolbar, then select the **Network Setup** tab.

Network Setup is divided into four sections:

- Basic Setup—settings that allow the 700wl Series system component to communicate with the network
- Advanced Setup—settings that configure client communication to and from the network

For an Access Control Server you can configure settings for:

- DHCP Network for NAT Clients—lets you configure the IP address range and DHCP lease time for the internal DHCP server used to provide private IP addresses for clients that should receive NAT'ed addresses.
- MAC Address Spoofing Detection—lets you configure the 700wl Series system to detect when the same MAC address appears on multiple Access Controller ports a specified number of times within a defined time period.

For 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 Polling—lets you set the interval for polling an idle client, and the time-out after which an idle client will be disassociated from the Access Controller.
- IP Broadcast Forwarding—lets you specify ports to which broadcast traffic should be forwarded
- SSL Setup (Integrated Access Managers and Access Control Servers)—lets you create a certificate signing request and load a signed certificate you receive from a Certificate Authority (CA)
- HTTP Proxy (Integrated Access Managers and Access Controllers)— lets you configure a proxy server for HTTP requests

The Basic Setup and Advanced Setup tabs appear for both Access Control Servers and Access Controllers. The SSL tab appears only for an Access Control Server or Integrated Access Manager. The HTTP Proxy tab appears only for the Access Controller or Integrated Access Manager.

The **Save** and **Cancel** buttons operate across all sub-tabs under the Network Setup page:

- **Save** saves all changes from all sub-tabs. You can move between sub-tabs and the changes you make on each page are preserved until you save or cancel.
- **Cancel** discards all changes you have made on any of the sub-tabs since the last Save.

The **Reset to Defaults** button resets the fields on the current sub-tab to their default values. These changes are not immediately saved, however. You must click **Save** to save them.

The Basic Setup tab is the initial page that appears. Figure 6-8 shows the Basic Setup tab of the Network Setup page, for an Integrated Access Manager. The Integrated Access Manager is used as an example in this section because it includes all the configuration options for both the Access Control Server and the Access Controller.

The network settings for each component are specific to that component; different Access Controllers can have different settings.

A concise version of the System Components List appears at the left of the page. You can open or close its folders to streamline the display of components. You use the System Components List to select the component you wish to configure.

Network Communication—the Basic Setup Tab

To configure the basic network communication settings for a 700wl Series system component, do the following:

- Step 1.** Under the network icon, click the **Network Setup** tab to display the Basic Setup tab, as shown in Figure 6-8.

Figure 6-8. Network Setup: Basic Setup page for an Access Control Server

The screenshot displays the HP ProCurve Network Setup interface. At the top, the HP logo and 'invent' tagline are visible. The user is logged in as 'admin' with the IP address 192.168.10.82. The main navigation bar includes 'System Components', 'Network Setup', 'Interfaces', 'SNMP', and 'Date & Time'. The 'Network Setup' section is active, showing 'Equipment' as 'Campus Access Control' with IP 192.168.10.82. The 'Basic Setup' tab is selected, and the configuration page is titled 'Network Setup'. On the left, a 'System Components List' shows 'Campus Access Control' selected. The main configuration area includes a 'Configure' dropdown set to 'Using DHCP', and fields for 'Hostname', 'Domain Name' (xyzcorp.com), 'IP Address' (192.168.10.82), 'Subnet Mask' (255.255.255.0 /24), 'Gateway' (192.168.10.1), 'Primary DNS' (192.168.2.248), 'Secondary DNS' (192.168.10.231), 'Primary WINS' (192.168.2.247), and 'Secondary WINS'. At the bottom, there are 'Save', 'Reset to Defaults', and 'Cancel' buttons.

- Step 2.** In the System Components List at the left, select the component you want to configure. If you have a redundant peer configured, there may be two Access Control Servers shown.

The fields that appear on the Basic Setup page are slightly different depending on whether the component is an Access Control Server, Integrated Access Manager, or Access Controller.

Configuring the Network

Edit the contents of the fields on this page as appropriate. The fields and their settings are defined in Table 6-5.

Table 6-5. Basic Setup tab fields

Field	Description
Configure	<p>A drop-down list you use to specify how this component gets its IP address.</p> <ul style="list-style-type: none">• Select Using DHCP to have the unit request its IP address, subnet mask, gateway, DNS server and WINS server IP addresses from the DHCP server.• Select Manually to enter a static IP address and configure the other settings directly as well. <p>If you choose Using DHCP, the system will request its IP address, subnet mask, gateway, DNS server and WINS server IP addresses from the DHCP server. In this case, the rest of the address fields on this page are filled in automatically.</p> <p>Note: <i>If you are changing from a static IP address to use DHCP, do not change the values in the following fields (e.g. IP address or default gateway). They will be cleared and reset appropriately when you submit your changes.</i></p>
Hostname	<p>A fully qualified hostname for this system of no more than 50 characters. Assigning a hostname is optional.</p> <p>The hostname must be fully-qualified, for example: <i>acserver.ca.xyzcorp.com</i>. 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.</p> <p>Note: <i>HP recommends creating a hostname. Using a hostname prevents client users from getting SSL warnings about an unknown SSL certificate when they first access the logon page.</i></p>
Domain Name	<p>The name of the domain in which this system resides, for example <i>xyzcorp.com</i>. This will be used as the default domain, and appended to any host names that are not fully-qualified.</p>
DHCP Server IP (Appears only if this is an Access Controller or Integrated Access Manager)	<p>IP address of an external DHCP server used to provide real IP addresses for clients.</p> <p>This is required <i>only</i> if the DHCP server is not on the same subnet as this Access Controller or Integrated Access Manager, and is not reachable through a DHCP forwarding router.</p> <p>Leave blank if the DHCP server is on the same subnet as this Access Controller.</p> <p>Note: <i>You must enter a DHCP server IP address if you plan to specify IP subnet ranges for individual ports on the Advanced Setup page.</i></p>
<p>The following fields should be filled in only if you have selected Manually for the Configure setting. If you selected Using DHCP, these will be filled in automatically.</p>	
IP Address	<p>The IP address of this 700wl Series system component.</p> <p>Note: <i>If you have selected Using DHCP above, you cannot modify this field.</i></p>
Subnet Mask	<p>The subnet mask that defines the subnet for this unit.</p> <p>Note: <i>If you have selected Using DHCP above, you cannot modify this field.</i></p>
Gateway	<p>The IP address of the gateway (default router) to the network</p> <p>Note: <i>If you have selected Using DHCP above, you cannot modify this field.</i></p>
Primary DNS	<p>The IP address of the primary DNS server</p>

Table 6-5. Basic Setup tab fields

Field	Description
Secondary DNS	The IP address of the secondary DNS server
Primary WINS	The IP address of the primary WINS server
Secondary WINS	The IP address of the secondary WINS server

Step 3. Click **Save** to save your settings.

To restore these fields to the original default settings, click **Reset to Defaults**. You must then Save to actually have the defaults take effect.

To abandon your changes and revert to the current settings, click **Cancel**.

Note: **Save** saves all changes made on any of the sub-tabs since the last Save. **Cancel** discards all changes on all sub-tabs since the last save.

Advanced Network Configuration—the Advanced Setup Tab

Step 1. From the Network Setup tab, click the **Advanced Setup** tab.

The Advanced Setup page appears. Figure 6-9 shows the Advanced Setup tab for an Integrated Access Manager, which includes all the tabs for both an Access Control Server and an Access Controller.

Step 2. From the System Components List, select the system to configure.

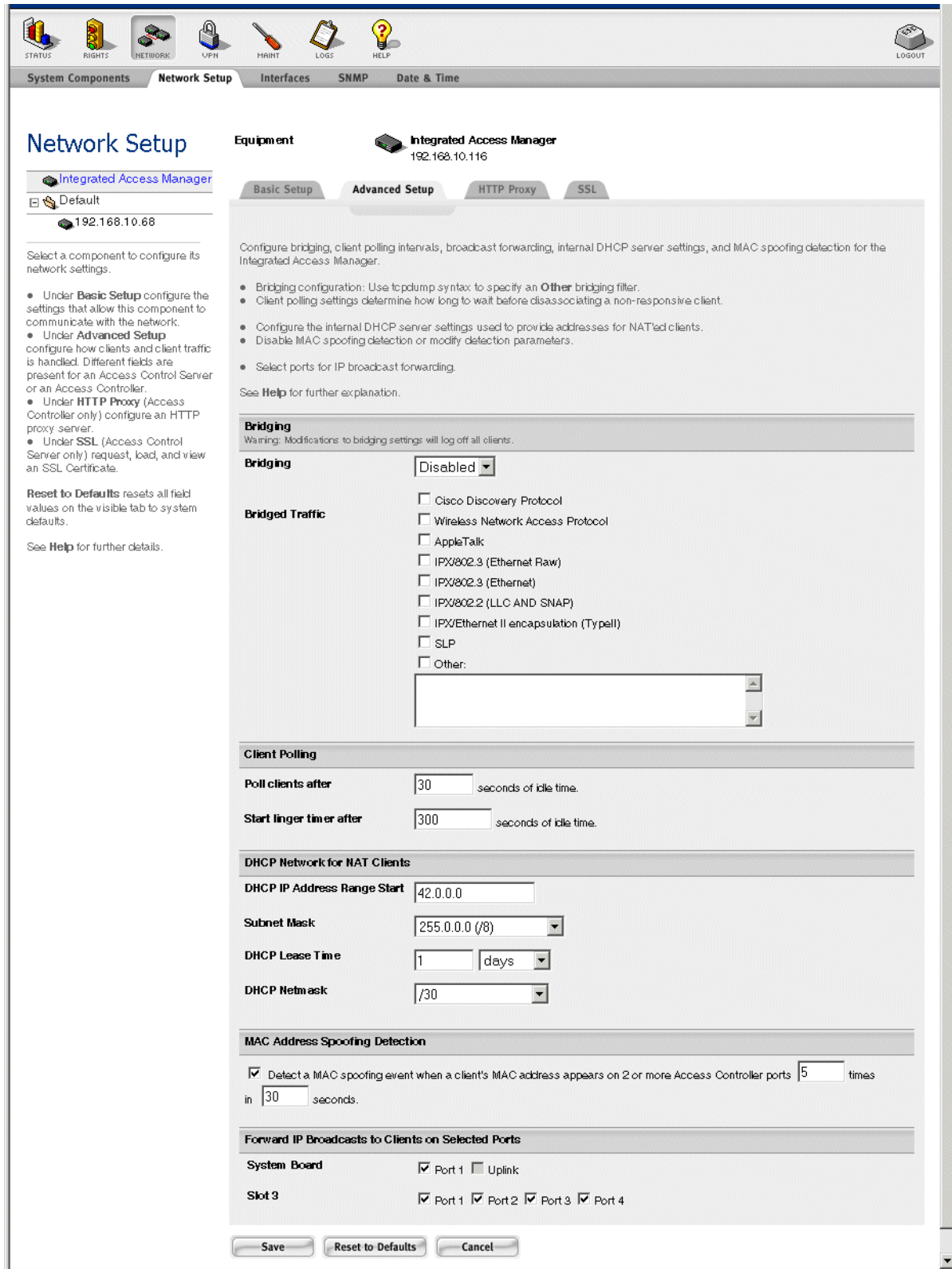
Step 3. When you have finished making your changes, click **Save**.

To restore these fields to the original default settings, click **Reset to Defaults**. You must then Save to actually have the defaults take effect.

To abandon your changes and revert to the current settings, click **Cancel**.

Note: **Save** saves all changes made on any of the sub-tabs since the last Save. **Cancel** discards all changes on all sub-tabs since the last save.

Figure 6-9. Network Setup: Advanced Setup page for an Integrated Access Manager



Access Control Server Configuration Advanced Options

The following settings appear on this page if you are configuring an Access Control Server or an Integrated Access Manager. They do not appear if you are configuring an Access Controller.

DHCP Network for NAT Clients

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, or days. 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 DHCP Subnet** setting.

Note: It can take some time for this configuration change to be propagated to each Access Controller. Clients that associate within this time frame may still receive an IP address from the old address range. It is recommended that you make this type of change during periods when client activity is at a minimum.

MAC Address Spoofing Detection

MAC Address spoofing occurs when someone impersonates a legitimate client by taking over their MAC address. You can configure the 700w1 Series system to detect the situation where the same MAC address appears on multiple Access Controller ports within a defined time period. If the same client appears on different ports a specified number of times within a specified time interval, the client is considered to have been spoofed, and all instances of that client are logged off the system. You can configure the number of times a client must appear, and the time interval within which this must occur in order for a client to be assumed to be spoofed.

MAC address spoofing detection is enabled by default. To change the configuration of spoofing detection, or to disable it, do the following:

- Step 1.** 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 2.** Specify the time frame (in seconds) in which these appearances must occur. The default is 10 seconds.
- Step 3.** To disable MAC spoofing detection, click the checkbox. The default is that MAC address spoofing is enabled.

Access Controller Advanced Configuration Options

The following settings appear on this page if you are configuring an Access Controller or an Integrated Access Manager. They do not appear if you are configuring an Access Control Server.

Bridging

A 700w1 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 Access Controller to the clients. Bridging is disabled by default.

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

To **Enable Ethernet Bridging** for this Access Controller, do the following:

Step 1. From the **Bridging** drop-down field, select **Enabled**.

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

Table 6-6. Bridging options

Protocol	Description
Cisco Discovery Protocol	Enables CDP packets through this Access Controller. This Layer 2 protocol is used by Cisco network hardware and software to manage a network of Cisco devices.
Wireless Network Access Protocol	Enables WNMP packets through this Access Controller. This Layer 2 protocol is used by Symbol Technologies, Inc. network hardware to manage a network of Symbol devices.
AppleTalk	Enables AppleTalk packets to be passed through this Access Controller.
IPX/802.3 (Ethernet Raw)	Enables Novell 802.3 IPX Ethernet traffic
IPX/802.3 (Ethernet)	Enables IEEE standard 802.3 IPX traffic.
IPX/802.2 (LLC and SNAP)	Enables IPX traffic that includes the 802.2 Logical Link Control (LLC) header and the Subnetwork Access Protocol (SNAP) header.
IPX/Ethernet II encapsulation (Type II)	Enables IPX traffic encapsulated using the standard Ethernet 2 header
SLP (Service Location Protocol)	Enables Novell SLP traffic to be passed through this Access Controller/
Other:	Enables bridging of other Layer 2 traffic as specified in the text field that follows. You can create a traffic specification using arbitrary <code>tcpdump</code> syntax. Any traffic specifications (<code>tcpdump</code> -enabled packets) you enter here are in addition to those enabled by checking the options described above.

See Appendix B, “Filter Expression Syntax” for a description of the `tcpdump` syntax.

The following are the specifications in tcpdump syntax for the predefined bridging options:

Table 6-7. Tcpdump syntax for pre-defined bridging options

Traffic to enable	tcpdump syntax
CDP	ether [12:2] <= 1514 and ether dst 01:00:0c:cc:cc:cc
Wireless Network Access Protocol	ether [12:2] = 0x8781 and ether[0:4] = 0x01a0f8f0
Appletalk	ether[12:2] = 0x809b or ether[12:2] = 0x80f3 or (ether[12:2] <= 1500 and (ether[14:4] = 0xaaaa0308 and ether[18:4] = 0x0007809b) or (ether[14:4] = 0xaaaa0300 and ether[18:4] = 0x000080f3))
IPX/802.3 (Ethernet Raw)	ether[12:2] < 0x05ee and (ether[14:2] = 0xffff)
IPX/802.3 (Ethernet)	ether[12:2] < 0x05ee and (ether[17:2] = 0xffff or ether[22:2] = 0xffff)
IPX/802.2 (LLC AND SNAP)	(ether[12:2] < 0x05ee and ether[14:2] = 0xaaaa and ether[16] = 0x03) or (ether[12:2] < 0x05dd and ether[14:2] = 0xaa08 and ether[16] = 0x00)
IPX/Ethernet II encapsulation (Typell)	ether[12:2] = 0x8037 or ether[12:2] = 0x8137
SLP	udp dst port 427 and dst host 224.0.1.22

Note: You must also have a matching Allowed Traffic filter defined and enabled in the appropriate Access Policies to allow this type of traffic from a client. Allowed Traffic filters are pre-defined for CDP, WNMP, and Appletalk, so you only need enable them for the appropriate Access Policies. For IPX and SLP you must create an Allowed Traffic Filter with the same tcpdump string as is used for the bridging option.

Client Polling

After a client has been idle for a specified length of time (by default 30 seconds), the Access Controller polls the client with an ARP request to determine if it is still connected. If the Access Controller does not receive a response to repeated polling after a specified timeout interval (by default five minutes) the system disassociates the client.

The actual poll interval may be up to 2 times the configured interval—if the client responds to the ARP, the client is not considered idle. However, if the client is not sending any other traffic, then after the appropriate interval another ARP request is sent—but the actual interval between those ARPs will be the time taken for the ARP response plus the configured idle time interval.

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 a *linger timeout* for that client. The value of the linger timeout is defined in the Access Policy associated with the client. If the client has not re-established communication before the linger timeout expires, any active sessions belonging to the client are terminated. The client is not logged out by this action—whether it will need to reauthenticate depends on the authentication timeout specified in the Access Policy.

If the client re-establishes communication with any Access Controller before the linger timer expires, that Access Controller informs the Access Control Server and gets the previous definition of

Configuring the Network

the client's rights. Depending on the Wireless Data Privacy mechanism and the type of addressing in force, the client's existing sessions may be tunneled from the original Access Controller to the new Access Controller.

To change the client polling settings, do the following:

Step 1. To change the length of time a client must be idle to generate a client probe, change the value in the **Poll clients after** field. The default idle time 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 idle timer expires, the Access Controller probes the client by sending it an ARP request. If the client responds, it is no longer considered idle. If the client does not respond the Access Controller continues sending ARP requests at approximately the specified frequency as long as the client is idle, until the time-out is reached.

Step 2. To change the timeout counter, which determines when the client should be disassociated, change the number of seconds in the **Start linger timer after** field.

This counter determines how long a client must be idle before the Access Controller disassociates that client. The default is 5 minutes (300 seconds).

Note that the disassociate action can in itself take 30-40 seconds.

See "The Timeout Tab" on page 4-59 in Chapter 4, "Configuring Rights" for more information on the linger timer.

Forward IP Broadcasts

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.*

Automatic HTTP Proxy Server Specification

If your network uses 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, utilizing HTTP 1.0, allows you to enforce the use of an 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. In addition, the automatic HTTP proxy feature lets you filter the HTTP traffic and conditionally allow or deny specific HTTP connections.

You can specify an external proxy server, or the 700wl Series system can act as the proxy server and handle the traffic according to the configured ports and filters defined for each Access Policy.

The automatic HTTP Proxy feature is configured and enabled specifically for each Access Policy. This lets you specify the HTTP proxy feature only for selected Access Policies, if appropriate. You also can configure sets of proxy filters per Access Policy.

There are two steps to implementing the automatic HTTP proxy feature:

- Step 1.** You must configure the Proxy Server so the Access Controller knows where to redirect HTTP requests. This is done through the **HTTP Proxy** tab under Network Setup.
- Step 2.** Within an Access Policy, you configure a set of filters (Accept and Deny rules) that conditionally allow or deny specific HTTP connections, and specify the TCP ports that should be monitored for HTTP traffic. This is done as part of the configuration of the Access Policy. See “The HTTP Proxy Tab” on page 4-55 and “HTTP Proxy Filters” on page 4-75 for more information.

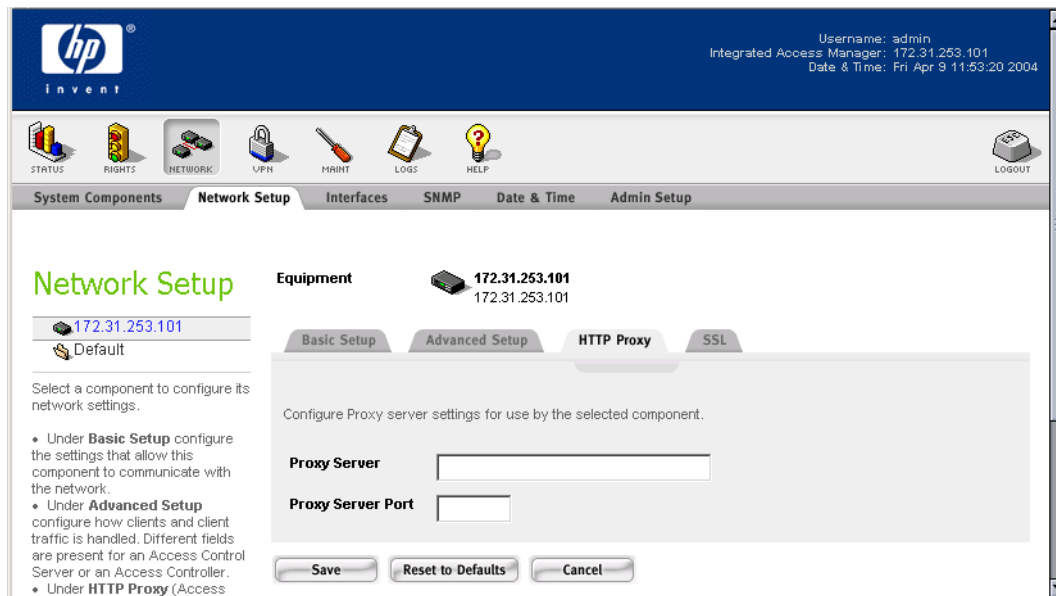
Note: If you do not configure a proxy server, but you configure and enable the automatic proxy feature within an Access Policy, the 700wl Series system will act as the proxy server, and will handle the traffic according to the configured ports and filters.

To configure the Proxy Server address, do the following:

- Step 1.** On the Network Setup page, select the **HTTP Proxy** tab.

The HTTP Proxy page for this Access Controller appears, as shown in Figure 6-10.

Figure 6-10. Network Setup: HTTP Proxy page (Integrated Access Manager or Access Controller only)



- Step 2.** Select the Access Controller for which you want to configure an HTTP proxy.

- Step 3.** In the **Proxy Server** field, type the IP address or host name of the Proxy Server to which HTTP traffic should be redirected. If a host name is entered, the Access Controller will perform a DNS lookup and keep a list of all returned IP addresses with that host name. If an IP address is not

Configuring the Network

available, the HTTP Proxy Server on the Access Controller will cycle to the next available IP address.

Step 4. In the **Proxy Server Port** field, type the TCP port number used for the proxy server.

Step 5. Click **Save** to have your changes take effect.

To restore these fields to the original default settings, click **Reset to Defaults**. You must then Save to actually have the defaults take effect.

To abandon your changes and revert to the current settings, click **Cancel**.

Note: **Save** saves all changes made on any of the sub-tabs since the last Save. **Cancel** discards all changes on all sub-tabs since the last save.

Once this has been done, you can go to the Rights Manager to configure and enable the automatic HTTP proxy for individual Access Policies.

SSL Certificate

With browser-based logon, users authenticate themselves to an Access Manager through an SSL-protected web interface. The 700w1 Series system comes with an SSL certificate issued by HP itself as the Certificate Authority (CA). When users access the logon page they receive a security alert warning of an untrusted certificate. To eliminate this warning you can replace the default SSL certificate with one signed by an external signing authority.

Note: *Chained or Intermediate certificates are not supported.*

Replacing the default SSL certificate with a custom certificate is a two-step process: First, you must generate a certificate signing request (CSR). You submit this CSR to an external signing authority, such as Verisign. They return a signed SSL certificate. You then upload this certificate onto the Access Control Server.

Step 1. On the Network Setup page select the Access Control Server in System Components List.

Step 2. Click the **SSL** tab.

The SSL page appears. See Figure 6-11

Figure 6-11. Network Settings: SSL Tab (Integrated Access Manager or Access Control Server only)

The screenshot displays the HP ProCurve Network Setup interface. At the top, the HP logo and 'invent' tagline are visible. The user is logged in as 'admin' with the IP address '192.168.10.116' and the date/time 'Tue Feb 10 18:35:10 2004'. The navigation menu includes 'System Components', 'Network Setup', 'Interfaces', 'SNMP', and 'Date & Time'. The 'Network Setup' section is active, showing 'Equipment' as 'Integrated Access Manager' with IP '192.168.10.116'. The 'SSL' tab is selected, displaying the following information:

Displays certificate information if a certificate is installed. To install a certificate, create a certificate signing request (CSR), submit it to your certificate authority, retrieve the signed certificate and load it here, then save the private key.

To restore a saved private key, Click **Save & Restore...**

Current Certificate	
Issued to	subject= /C=US/ST=California/O=Hewlett-Packard Company/CN=192.168.10.116/emailAddress=http://www.hp.com/go/hpprocurve
Issued by	issuer= /C=US/ST=California/O=Hewlett-Packard Company/CN=192.168.10.116 Certificate Authority/emailAddress=http://www.hp.com/go/hpprocurve
Valid Dates	notBefore=Feb 5 00:33:25 2004 GMT notAfter=Feb 3 00:33:25 2009 GMT
MD5 Fingerprint	MD5 Fingerprint=48:2D:84:7E:6B:6C:A3:E1:12:B6:E2:7A:83:4F:26:B6

Options

Generate CSR Generate a certificate signing request (CSR), then submit the request to your certificate authority (CA) to be signed.

Load Certificates After submitting a certificate signing request (CSR) to your certificate authority (CA), you will be issued a signed local certificate. Load the CA certificates here.

Save and Restore Private key Save and restore your SSL private key here

At the bottom of the page, there are three buttons: **Save**, **Reset to Defaults**, and **Cancel**.

The information at the top of the page shows information about the current certificate. Initially this will be the certificate generated and signed by HP ProCurve.

Note: The **Save** button on this page saves the changes you make to **any** of the sub-tabs under the Network Setup tab. If you **Reset to Defaults** to restore the default 700wl Series-provided certificate, you must **Save** to have that take effect. The other certificate-related functions have their own **Save** functions as appropriate on the pages that appear when you invoke those functions.

Requesting an SSL Certificate

To generate an SSL Certificate Signing Request (CSR):

Step 1. From the **SSL** tab, click **Generate CSR...**

The Generate SSL Certificate Signing Request page appears, as shown in Figure 6-12, in a separate browser window.

Figure 6-12. Input Page for Generating an SSL CSR

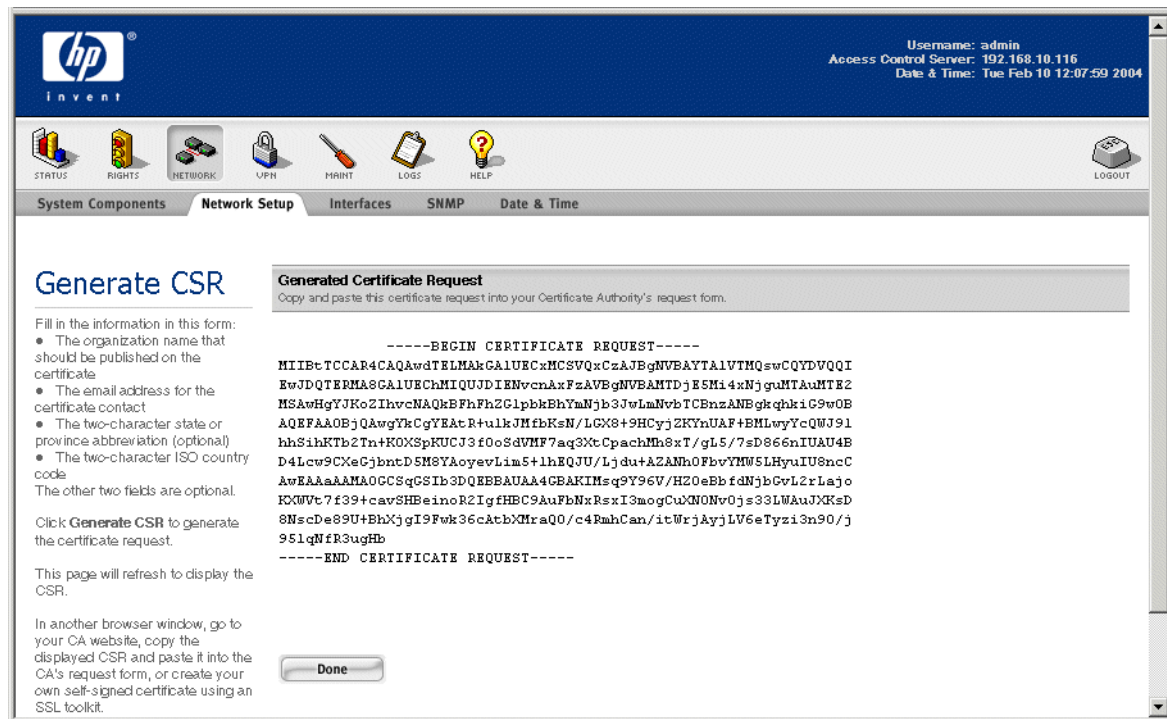
Step 2. Fill in all the entry fields:

- a. Type the organization name. This is the name that will be published on the certificate.
- b. Type the E-mail 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, *etc.*). 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 3. Click **Generate CSR**.

The page reappears with the Certificate Signing Request displayed, as shown in Figure 6-13.

Figure 6-13. The Certificate Signing Request



You can use this certificate signing request either to request a certificate from a CA, or to create your own self-signed certificate using an SSL toolkit, such as OpenSSL.

Step 4. You may be able to paste this signing request directly into a form on your CA's web site. To do so, connect to your CA's web site and begin the certificate request process. Copy the CSR (including the full *BEGIN* and *END* lines and all dashes) and paste it in the appropriate location.

When contacting an external signing authority such as Verisign, ask for an SSL signing request for an Apache modssl-based web server. A 40-bit certificate is all that is required.

Note: *Chained or Intermediate certificates are not supported. For example, if you obtain a certificate from Verisign, purchase the Secure Site certificate, not the Secure Site Pro certificate, which is not supported by the 700wl Series system.*

Step 5. Click **Done** to close this window.

Note: *The CSR is generated based on a private key. If the private key is lost or regenerated, certificates based on this CSR will become invalid. After generating the CSR, save the private key on your local system. The private key used to generate the CSR will then be recoverable after a factory reset or hardware swap. See "Save and Restore Private Key" on page 6-33.*

Loading the SSL Certificate

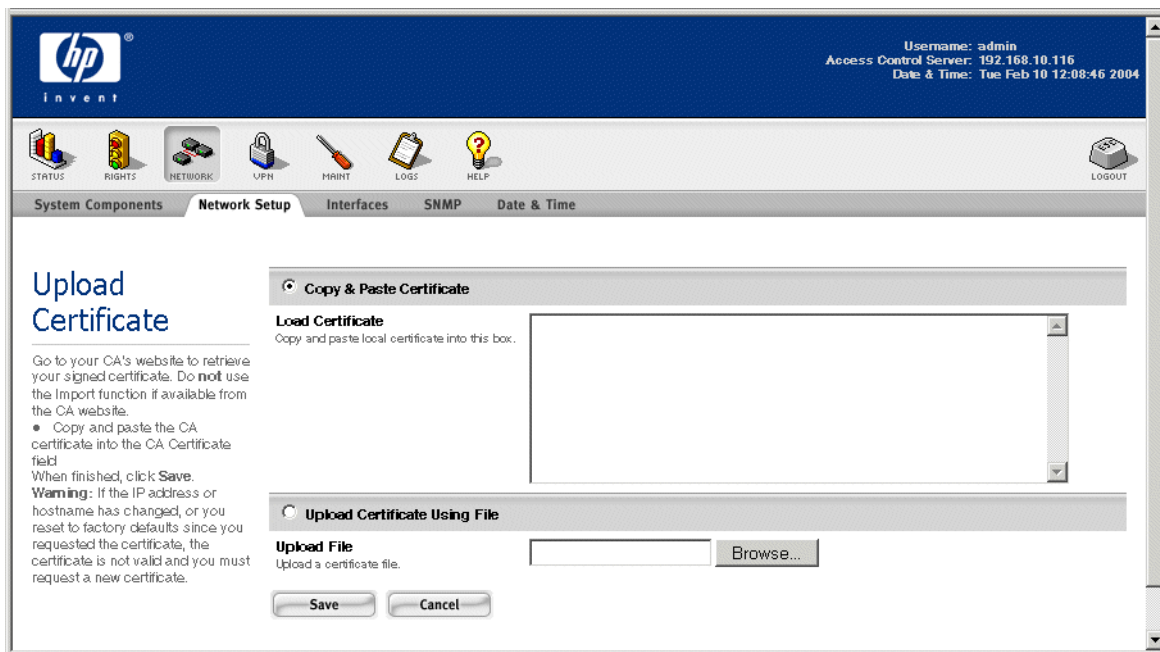
When you receive your certificate from the CA, you can either copy the certificate information and paste it into the field provided, or you can place the certificate in a file and upload the file. *Do not edit, add line breaks, or otherwise change any of the characters in the certificate, as this will corrupt the certificate.*

Step 1. Go to the Access Control Server's Network Setup page and click on the **SSL** tab.

Step 2. Click **Load Certificates...**

The Upload Certificate page appears, as shown in Figure 6-14, in a separate browser window.

Figure 6-14. Upload Certificate Page



Step 3. To paste the certificate from the CA, click the **Copy & Paste Certificate** radio button, and paste the certificate information into the text box provided.

To upload the certificate from a file, click the **Upload Certificate Using File** radio button, and type the filename and path for the file containing the CSR into the Upload File field. You can click on the **Browse...** button to locate the file.

Step 4. Click **Save** to save the certificate on the Access Control Server, and close the window.

The certificate will be loaded onto the Access Control Server, and will be used to authenticate the Access Control Server for SSL connections.

Note: *If you change either the hostname or IP address of the system, or if you reset to the factory defaults, the certificate is no longer valid. (A factory reset restores the default, 700wl Series-signed certificate). You must apply for a new certificate.*

Save and Restore Private Key

The CSR you generate is based on a private key. If the private key is lost or regenerated, any CSRs based on the original private key become invalid. After generating the CSR, you should save the private key on your local system. It can then be recovered after a factory reset or hardware swap.

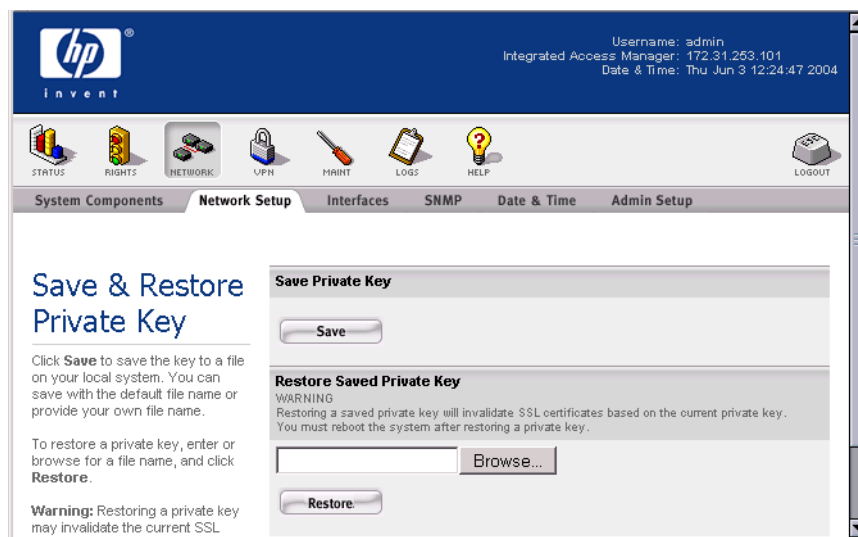
To save the current private key:

Step 1. Go to the Access Control Server's Network Setup page and click on the **SSL** tab.

Step 2. Click **Save & Restore...** under Save and Restore Private Key.

The Save and Restore Private Key page appears in a separate browser window. See Figure 6-15.

Figure 6-15. Save and Restore Private Key Page



Step 3. Under the Save Private Key heading, click **Save**. This also closes the window.

Depending on the operating system of your local system you will be asked where to save the private key file. The file is a small text file with a `.key` extension.

Caution: *The private key should be kept confidential. If someone else obtains access to your private key, your SSL certificate has been compromised.*

To restore a private key:

Step 1. Go to the Access Control Server's Network Setup page and click on the **SSL** tab

Step 2. Click **Save & Restore...** under the Save and Restore Private Key heading.

The Save and Restore Private Key page appears in a separate window. See Figure 6-15.

Step 3. Under the Restore Saved Private Key heading, enter the filename and path of the file containing the private key and click **Restore**. You can click on the **Browse...** button to locate the file.

Step 4. Click **Save** to save the key on the Access Control Server. This also closes the separate window.

Step 5. You must reboot the system after restoring a private key. Go to the **Shutdown/Restart** tab under the Access Control Server's Maintenance pages to reboot the system.

Configuring the Network

Caution: Restoring a saved private key will invalidate an SSL certificate based on the current (different) private key.

Restoring the Default SSL Certificate

If the private key is lost or the certificate is corrupted or invalidated, you can revert to the default SSL certificate issued by HP ProCurve itself as the Certificate Authority (CA).

To restore the default SSL certificate and private key, click **Reset to Default**, then click **Save**.

Note: **Save** saves all changes made on any of the sub-tabs since the last Save. **Cancel** discards all changes on all sub-tabs since the last save.

Configuring Network Interfaces

You use the Interfaces tab of Network Setup to configure the interfaces of your Access Controllers or Integrated Access Managers. You can configure:

- The transmission speed and duplex setting for each port on the Access Controller or Integrated Access Manager. You can also set the speed and duplex setting for the uplink port on an Access Control Server.
- The subnet address range for each Access Controller or Integrated Access Manager port.

Configuring the Port Speed and Duplex Settings

The Connection Type settings let you specify the speed and duplex setting for each I/O port. Port Settings are available on the **Speed/Duplex** tab of the Interfaces page for all system components.

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 (shown in parentheses). In Figure 6-17, on page 6-35, all ports are configured for autoselect (allowing automatic negotiation to determine the port settings). For the ports where no media is connected, the value in parentheses is **none**. 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).

The Connection Type field provides a drop-down list with the possible settings allowed for the port. Figure 6-16 shows an example of a drop-down list. The items in the list depend on the type of port.

Figure 6-16. Example of a Port Connection Type selection list

Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect
Port Connection Type	Ethernet autoselect

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

Step 1. On the Interfaces setup page select the Access Controller to configure.

Step 2. Click the **Speed/Duplex** tab.

The Speed/Duplex page for Access Controllers appears. See Figure 6-17.

Figure 6-17. Interfaces: Speed/Duplex Page

The screenshot shows the HP ProCurve web interface. At the top, the HP logo and 'invent' tagline are visible. The user is logged in as 'admin' with the IP address 192.168.10.116. The navigation menu includes System Components, Network Setup, Interfaces (selected), SNMP, and Date & Time. The main content area is titled 'Interfaces' and shows the configuration for an 'Access Controller' (IP: 192.168.10.68). The 'Speed/Duplex' tab is active. The page contains instructions on how to configure port connection types and a table for setting individual ports.

System Board	Port Connection Type
Uplink	Ethernet autoselect
Slot 1	Port Connection Type
Port 1	Ethernet autoselect
Port 2	Ethernet autoselect
Port 3	Ethernet autoselect
Port 4	Ethernet autoselect

Step 3. Select the connection type from the list provided in the drop-down list.

Configuring the Network

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 6-17, there is no setting for 100baseTX half-duplex. You must specify 100baseTX and allow the port to negotiate for half-duplex.

Step 4. Click **Save**.

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

To abandon your changes and revert to the current settings click **Cancel**.

Note: The port configuration process takes several seconds to take effect. When you initially return to the **Speed/Duplex** tab, 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 Subnet IP Address and Subnet Netmask

The Port Subnet IP Address and Port Subnet Netmask lets you specify an subnet address range for each Access Controller 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.
- It defines the range of valid IP addresses for clients using an Access Policy with a NAT setting of **When Necessary** (see "The Settings Tab" on page 4-45 in Chapter 4, "Configuring Rights"). 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.

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.

The example in Figure 6-18 shows an Access Controller 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 700w1 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 760w1 or Access Controller 720w1, depending on your system configuration.

Up to twelve downlink ports and one uplink port may be displayed for an Integrated Access Manager 760w1 or Access Controller 720w1, depending on the system configuration. Four downlink ports and the uplink port are displayed for an Integrated Access Manager 760w1 or Access Controller 720w1.

Note: The *Broadcasting* section on the *Advanced Setup* tab under *Network Setup* 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 on a 700wl Series system) is now a downlink port, then that port **will** appear on this page. The port being used as the uplink port will not appear.

To configure subnet addresses for Access Controller ports:

Step 1. On the Interfaces setup page select the Access Controller to configure.

Step 2. Click the **Subnet** tab.

The Subnet page for Access Controllers appears. See Figure 6-18.

Figure 6-18. Interfaces: Subnet Settings Page

The screenshot shows the HP ProCurve Management and Configuration interface. The top navigation bar includes 'System Components', 'Network Setup', 'Interfaces', 'SNMP', and 'Date & Time'. The 'Interfaces' section is active, showing 'Access Controller' selected. The 'Subnet' tab is selected, displaying a table for configuring port subnet IP addresses and netmasks.

System Board	Port Subnet IP Address	Port Subnet Netmask
Uplink	n/a	n/a
Slot 1	Port Subnet IP Address	Port Subnet Netmask
Port 1	<input type="text"/>	240.0.0.0 (/4) <input type="button" value="v"/>
Port 2	<input type="text"/>	240.0.0.0 (/4) <input type="button" value="v"/>
Port 3	<input type="text"/>	240.0.0.0 (/4) <input type="button" value="v"/>
Port 4	<input type="text"/>	240.0.0.0 (/4) <input type="button" value="v"/>

Buttons at the bottom: Save, Reset to Defaults, Cancel.

Step 3. Configure the port settings as appropriate, by entering a starting IP address and selecting a netmask from the drop down list in the Netmask field for each port.

Step 4. Click **Save**.

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

To abandon your changes and revert to the current settings click **Cancel**.

Note: There may be a short delay before these changes take effect.

Note: There are no restrictions on the IP addresses that can be used for port settings in relationship to the Access Controller's IP address. However, your upstream routers must have static routes

Configuring the Network

configured to support routing the addresses you have configured for your ports through the Access Controller 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 SNMP

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

The 700wl Series system SNMP module enables 700wl Series system components 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. The four HP ProCurve Secure Access 700wl Series MIBS are available from the Software and Downloads section of the HP ProCurve support web site at www.hp.com/go/hpprocurve. The four MIBS are: HP-BASE-MIB.txt, HP-SYSTEM-MIB.txt, HP-IF-EXT-MIB.txt, and HP-MEMPROC-MIB.txt.*

To configure SNMP for the 700wl Series system:

Step 1. Click the **SNMP** tab from any page in the network configuration module.

The SNMP page is displayed, as shown in Figure 6-19.

Figure 6-19. SNMP Page

The screenshot shows the HP ProCurve management interface. At the top, there is a blue header with the HP logo and 'invent' text. On the right, it displays 'Username: admin', 'Access Control Server: 192.168.10.116', and 'Date & Time: Tue Feb 10 12:16:09 2004'. Below the header is a navigation bar with icons for STATUS, RIGHTS, NETWORK, UPN, MAINT, LOGS, HELP, and a LOGOUT button. The main content area is titled 'SNMP' and shows configuration options for the 'Access Control Server' component. The 'SNMP' status is currently set to 'Disabled'. Other fields include 'SNMP Access Mode' (Read Only), 'Community Name' (public), 'SNMP Port' (161), 'Contact Info', and 'Trap IP Addresses'. There are also four empty fields for 'SNMP Manager 1' through 'SNMP Manager 4'. At the bottom, there are 'Save', 'Reset to Defaults', and 'Cancel' buttons.

Step 2. Select the system component for which you want to enable SNMP from the System Components List.

Step 3. SNMP is disabled by default. Select **Enabled** from the SNMP drop-down menu to enable SNMP. This will enable SNMP for the selected component.

Note: Enabling SNMP allows Read-only access to the device as indicated by the value in the **SNMP Access Mode** field.

Step 4. Type the appropriate read **Community Name**.

The default name is `public`; you should change it to match the read community name configured for your SNMP manager.

Step 5. 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 6. Type your **Contact Info**. Typically, this is the Network Administrator's name, E-mail address, or phone. This will be saved in the `sysContact` MIB object.

Step 7. In the **Trap IP Addresses** fields, type the IP address of up to two systems that should receive traps from the 700w1 Series system. Enter each IP address in a separate entry field.

Configuring the Network

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.

You can download the HP ProCurve MIBs from the HP ProCurve support web site at www.hp.com/go/hpprocurve.

Step 8. Type up to four **Manager** IP addresses in the fields provided.

These are the addresses of SNMP management consoles that are authorized to request information.

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 9. Click **Save** to save your settings.

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

To abandon your changes and revert to the current settings click **Cancel**.

Setting the Date and Time

Accurate time and date reporting is necessary for logs and for troubleshooting. Accurate and synchronized time and dates across multiple units is especially important. For example, if the date and time of your Access Control Server and Access Controller are not synchronized, you may see negative values for a client's Idle Time in the Client Status display.

You use the Time and Date page to set the time zones and to set the date and time, either manually or using a network time server. You can set the date and time separately for each system component, but you should ensure that they are synchronized.

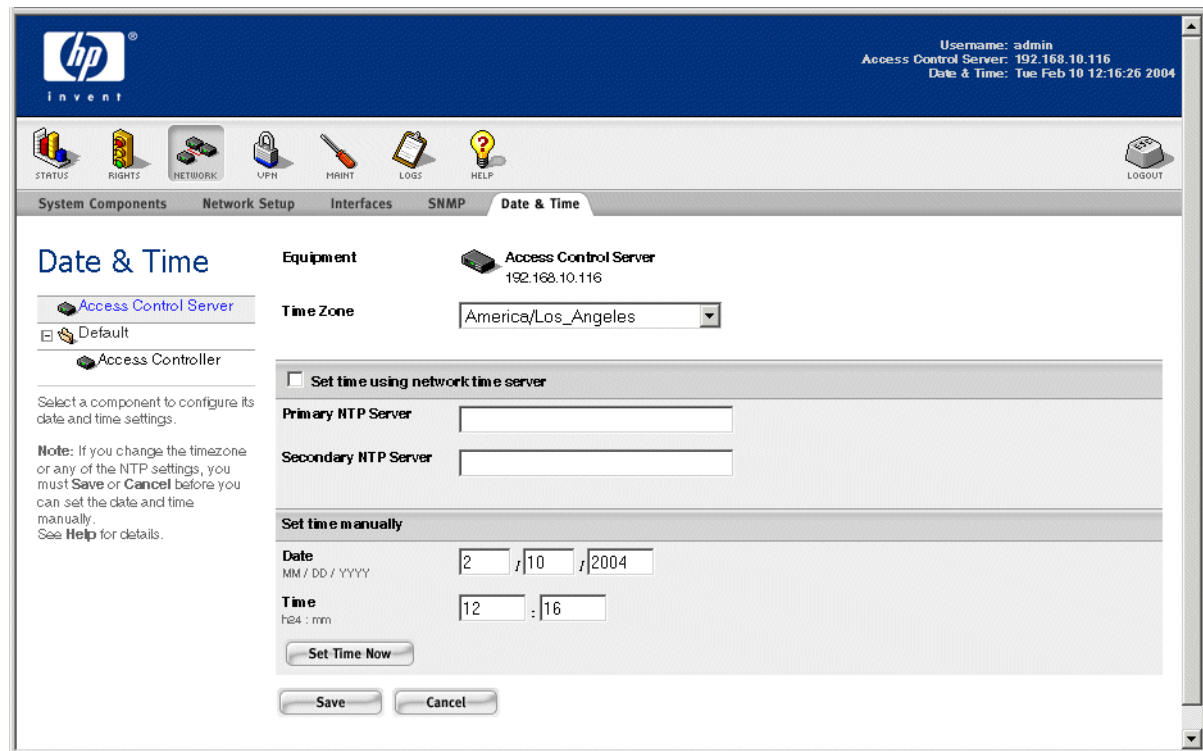
Note: You can change the time zone and set or modify the NTP server configuration in a single operation, **or** you can change the time manually. However, once you make a change to either the time zone or the NTP settings, you will not be able to change the date and time until you save (or cancel) the time zone and NTP changes.

To configure the time and date for one or more components, do the following:

Step 1. Click the **Date & Time** tab from any page in the Network module.

The Date & Time page appears. See Figure 6-20.

Figure 6-20. Date & Time Page



Step 2. Using the System Components List on the left select the component for which you wish to set the date and time.

You can select an Access Control Server, a single Access Controller, or a folder. If you select a folder, the date and time settings you enter will be applied to all the Access Controllers in that folder.

You can configure the system to get the date and time from a Network Time Protocol (NTP) server or you can set it manually. You can also make a date and time adjustment manually even if you have the system configured to get time from an NTP server.

- » To change the time zone setting, select the time zone that is appropriate for your location from the drop-down list in the **Time Zone** field, then click **Save**.
- » To configure the system to get the time from an NTP server:
 - a. Click the checkbox next to **Set time using network time 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.
 - d. Click **Save** to save your settings.

To abandon your changes, click **Cancel**.
- » To set the time manually:
 - a. Enter the desired date and time in the date and time fields. (You do not need to disable the NTP feature to change the time manually).

Configuring the Network

The format for the date is MM/DD/YYYY. For example, June 4, 2003 would be entered as 06/04/2003.

The format for the time is HH:MM, using a 24 hour clock. For example, 6:23 PM would be entered as 18:23.

- b. Click **Set Time Now** to set the date and time according to settings you entered.

Note: *If you have made any changes to the time zone or NTP server settings, you cannot manually change the time settings until you have saved or canceled the time zone or NTP 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 use. 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 potential disruptions.*

Setting Up Administrators

The 700w1 Series system provides one built-in administrator that has Super Administrator capabilities. The Super Administrator can also create additional administrator users, some of which can have restricted access capabilities.

The 700w1 Series system supports three types of administrators:

- Super Administrators, who can perform all administrative functions for all components of a 700w1 Series system. This includes all network configuration, maintenance such as upgrades, backups, reboots, and rights configuration. You can create 20 administrator users (in addition to the built-in administrator). A Super Administrator can also access any of the connected system components using the CLI. Any Super Administrator can create, modify or delete other administrator users.
- Network Administrators, who can perform network configuration functions, such as configuring IP addressing, interface configuration, date and time settings, SNMP access, and performing software updates and backups, for all connection components of a 700w1 Series system. A Network Administrator cannot perform any rights configuration, and can only modify his/her own administrator password.
- Policy Administrators, who can perform any functions under the Rights Manager, such as creating, modifying or deleting Access Policies and Authentication Policies, configuring Authentication Services, adding users, setting up Custom logon pages. A Policy Administrator cannot do any network configuration or maintenance functions, can only modify his/her own administrator password, and cannot access the CLI.

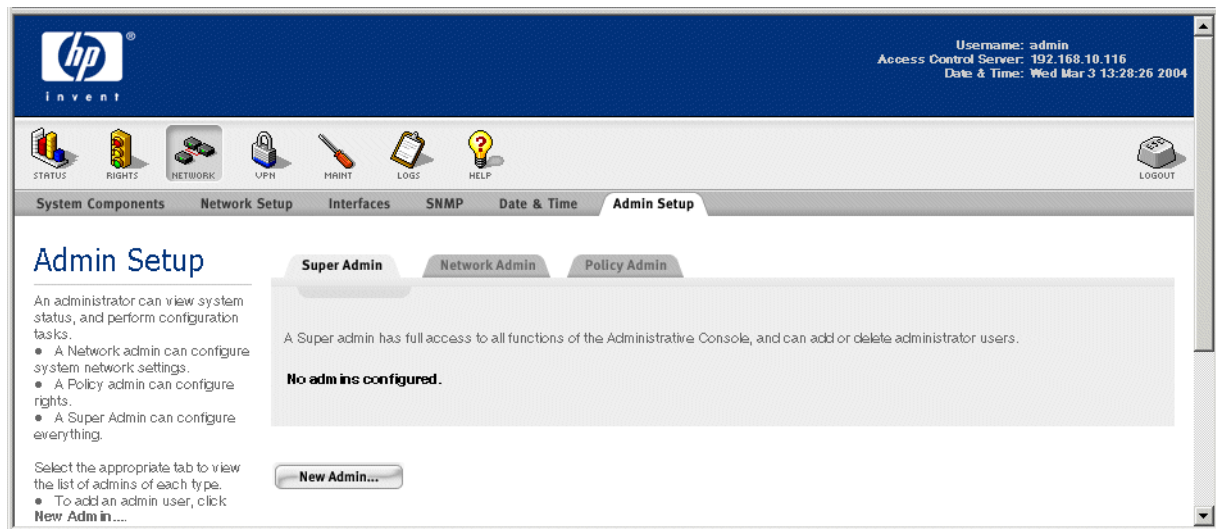
To configure an administrator user, do the following:

- Step 1.** Click the **Admin Setup** tab from any page in the Network module.

The Admin Setup page appears (see Figure 6-21).

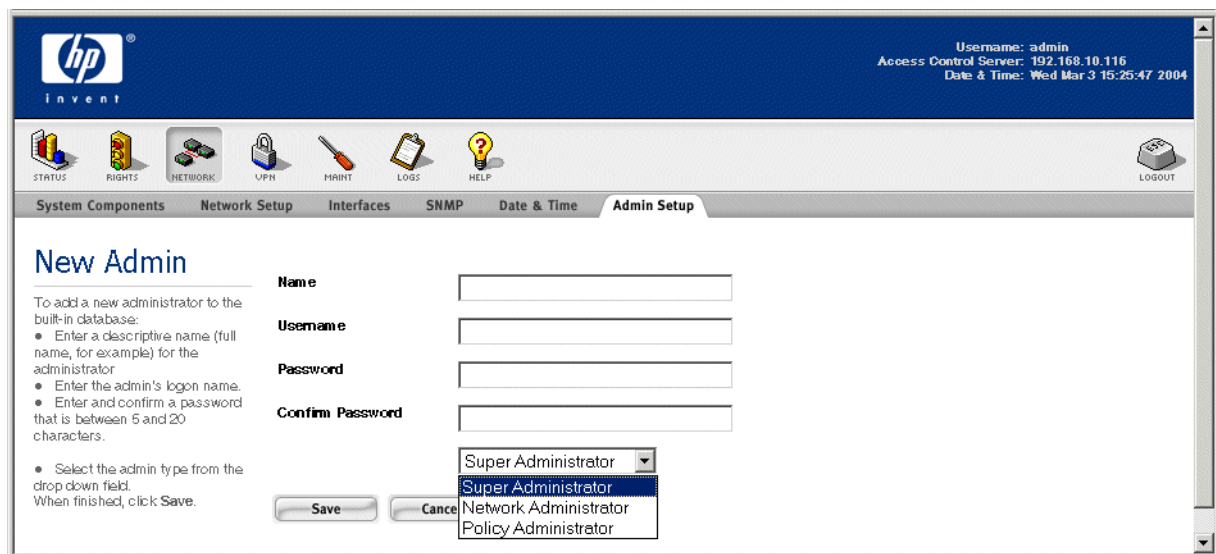
Note: *Only a Super Administrator will see this page; a Network Administrator or Policy Administrator will see the Edit Admin page for their own administrator account.*

Figure 6-21. Admin Setup page



Step 2. Click **New Admin...** The New Admin page appears (see Figure 6-20).

Figure 6-22. Admin Setup page



Step 3. Fill in the fields as required (see Table 6-8) and select the administrator type from the drop-down menu.

Table 6-8. New/Edit Admin Fields

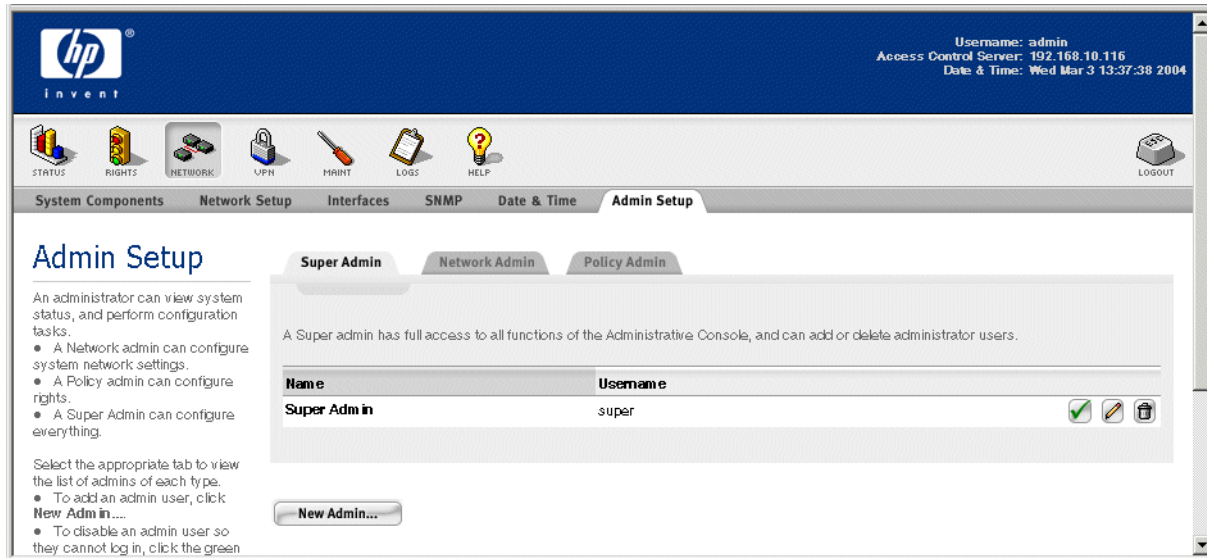
Field	Description
Name	A descriptive name that identifies the Administrator. It can be the administrator's full name or any other meaningful name. This name may have up to 32 characters. Any 7-bit characters are allowed.
Username	The administrator's logon ID. A username may have up to 50 characters. Any 7-bit characters are allowed.
Password	The password associated with the administrator's logon name. The password must be at least five, and no more than 20 characters in length.
Confirm Password	The same password, entered a second time as a confirmation.

Step 4. Click **Save** to add this administrator, or **Cancel** to abandon your changes.

Editing an Administrator's Settings


Once an administrator has been added, it appears in the list under the appropriate tab—Super Admin, Network Admin, or Policy Admin. Figure 6-23 shows an example.


Figure 6-23. Admin Setup with existing admins listed



A Super Administrator can edit, enable or disable, or delete any administrator account.

Note: The built-in administrator name and password for a 700wl Series system component is set on the System Component Edit page. It cannot be changed through the Admin Setup function. See "Configuring an Access Control Server" on page 6-3, "Configuring an Integrated Access Manager" on page 6-7, or "Configuring Access Controllers" on page 6-10 for more information.

- To edit an administrator account, click the administrator's Name or Username, which are links to the Edit Admin page, or click the Pencil icon at the right of the row. The Super Administrator can change any of the settings for an administrator.
- By default, a newly-added administrator account is enabled, meaning that the administrator can logon to the Administrative Console with the Username and password as set by the Super Administrator. This is indicated by a green check button () to the right of the administrator Username.

Disabling an administrator account means that the administrator will not be allowed to log on to the Administrative Console (or the CLI, if it is a Super Administrator or Network Administrator). This is indicated by a red "prohibited" symbol button () to the right of the administrator Username.

- To disable an administrator, click the green check button. It will change to the red "prohibited" symbol.
- To enable an administrator, click the red "prohibited" button. It will change to the green check.
- To delete an administrator, click the trash can button at the far right of the row.

Editing Your Administrator Password

Any Administrator, including a Network Administrator or Policy Administrator, can change his or her own password. For example, a Policy Administrator cannot perform any of the functions under the Network area, except to change her password.

To change your own administrator password, do the following:

Step 1. If you are a Network Administrator, click the **Network** icon, then the **Admin Setup** tab. The Edit Admin page appears, with your administrator account information shown.

If you are a Policy Administrator, click the **Network** icon. The Edit Admin page appears immediately, since it is the only function you can perform under the Network icon.

Step 2. Type your new password (and type a second time to confirm). You cannot change any other fields in the form.

Step 3. Click **Save** to save your changes, or **Cancel** to abandon them.

SETTING UP WIRELESS DATA PRIVACY

This chapter explains how to configure the global settings for the security protocols. The topics covered in this chapter are:

Overview of Wireless Data Privacy	7-1
Wireless Data Privacy Setup	7-2
IPSec Certificate Configuration	7-5
IP Address Assignment for Tunneling	7-11

Overview of Wireless Data Privacy

Wireless Data Privacy is an optional security feature of the 700wl Series system 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 plus IPSec, tunnel mode IPSec, and SSH.

To use one of these protocols for Wireless Data Privacy, there are three basic conditions that must be met:

- The protocol must be enabled and configured appropriately for the 700wl Series system as a whole.
- The use of individual security protocols (the encryption policy that pertains to specific clients) must be specified (required or allowed) in the relevant Access Policies.
- The appropriate Wireless Data Privacy client software must be installed and configured on the client systems that expect to make use of those protocols.

All the security protocols can be enabled or disabled globally without having to change the settings in the individual Access Policies.

For IPSec and the other tunneling protocols there are some settings that must be configured centrally, either across the 700wl Series system as a whole, or per Access Controller:

- For IPSec, the configuration of the IKE Authentication method and IKE and ESP encryption and integrity algorithms is done centrally on the Access Control Server for the 700wl Series system as a whole
- For the tunneling protocols (IPSec, PPTP and L2TP) the configuration of IP addressing used in setting up inner tunnel addresses is done on a per-Access Controller basis.

The global security settings are set under the VPN pages of the 700wl Series system Administrative Console, and are discussed in this chapter.

Setting up Wireless Data Privacy

The encryption policy that defines how encryption applies to a specific client is determined through the Access Policy that defines rights for that client. The Access Policy can specify that encryption is required, that it is allowed but not required, or that it is disabled. It also specifies which encryption methods can be used. These settings are specified when you create an Access Policy. See “Access Policies” in Chapter 4, on page 4-39 for a detailed discussion of configuring encryption in an Access Policy.

Client configuration is discussed in detail in the *700wl Series system Wireless Data Privacy Configuration Guide*, available on the HP ProCurve Documentation CD or on the 700wl Series system Technical Support web site. This same manual contains a more in-depth discussion of encryption protocols and their use with the 700wl Series system.

Wireless Data Privacy Setup

The Wireless Data Privacy page provides settings that determine the encryption protocols that can be used with the 700wl Series system. The security protocols can be enabled or disabled globally on this page, affecting all components of the 700wl Series system.

Configuration of IPSec on the 700wl Series system consists of selecting and setting up the IKE authentication method (shared secret or certificate) and noting which algorithms the 700wl Series system is prepared to negotiate. It is up to the client system to propose algorithms, and the 700wl Series system either agrees or not.

IPSec configuration is handled centrally for the entire 700wl Series system. IPSec usage is enabled within Access Policies on a policy-by-policy basis.

The configuration of IPSec involves several steps:

- Specifying the IKE authentication method (Public Key certificate or IPSec shared secret)
- Requesting and installing a signed local certificate and a certificate from the Certificate Authority (CA), or setting the IPSec shared secret
- 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, click the **VPN** icon in the Navigation bar at the top of the Administrative Console. This displays the Wireless Data Privacy tab, as shown in Figure 7-1.

Figure 7-1. The Wireless Data Privacy tab

Wireless Data Privacy

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

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

For IPSec, select the Authentication method:

- To use a certificate, go to the **Certificates** tab to obtain and load a certificate.
- To use a shared secret, enter and confirm the secret string.

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

When finished, click Save.

Global Wireless Data Privacy Configuration

Encryption Protocols:

- Enable IPSec
 - Enable L2TP+IPSec (requires IPSec)
- Enable PPTP
- Enable SSH

Configuration for IPSec

IKE Authentication Method

- Public Key Certificate
- IPsec Shared Secret: Confirm:

IKE Encryption

- DES 3-DES Blowfish CAST

IKE Integrity

- SHA-1 MD5

IKE Diffie-Hellman

- Group 1 Group 2 Group 5

ESP Encryption

- DES 3-DES AES Blowfish CAST Null

ESP Integrity

- SHA-1 MD5 Null

Save Reset to Defaults Cancel

Global Wireless Data Privacy Configuration

Select the Wireless Data Privacy protocols you want to enable for the 700wl Series system. By default, all protocols are disabled.

Enabling a security protocol makes it available for use by clients within the constraints of the security settings embodied in the Access Policies for those clients.

- An encryption protocol that is enabled globally, but that is not allowed or required within an Access Policy will not be available for use by clients whose rights are controlled by that Access Policy.
 - An encryption protocol that is disabled globally will not be available to clients, even if the Access Policy allows or requires that protocol. If an Access Policy requires a protocol that is disabled, clients affected by that Access Policy will not be able to connect to the 700wl Series system.
- » To enable an encryption protocol, click the checkbox to turn on the check.

Note: To enable L2TP+IPSec, you must first select IPSec. The L2TP+IPSec checkbox is then available for selection.

Configuration for IPSec

Under this heading, select or enter data into the fields as described in Table 7-1 below.

Setting up Wireless Data Privacy

The fields and settings under the Configuration for IPSEC heading of the Wireless Data Privacy tab are as follows:

Table 7-1. IPSEC configuration settings

Field	Description
IKE Authentication Method	<p>Select the IKE Authentication Method you plan to use:</p> <ul style="list-style-type: none">• To use certificate-based authentication, click Public Key Certificate. If you elect to use this method, you will need to configure a public key certificate. You can do this under the Certificates tab after you have finished with the IPSEC setup. See "IPSEC Certificate Configuration" on page 7-5 for details on setting up these certificates.• To use shared secret-based authentication, click IPSEC shared secret, and type and confirm your shared secret in the fields provided. This defines 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. The shared secret must be a minimum of five characters. Note: <i>The IPSEC shared secret must be known by every IPSEC client. Using a shared secret makes the system vulnerable to man-in-the-middle attacks. Therefore this method is not recommended. It is provided as a convenience for sites who cannot or choose not to use certificate-based authentication.</i>
IKE Encryption	<p>Select the appropriate IKE encryption algorithms. The 700wl Series system supports the following algorithms:</p> <ul style="list-style-type: none">• DES• 3DES• Blowfish• CAST <p>The default is DES and 3DES selected.</p>
IKE Integrity	<p>Select the appropriate IKE integrity algorithms. The 700wl Series system supports the following algorithms:</p> <ul style="list-style-type: none">• SHA-1• MD5 <p>The default is both SHA-1 and MD5 selected.</p>
IKE Diffie-Hellman	<p>Select the appropriate IKE Diffie-Hellman algorithms. The 700wl Series system supports Groups 1, 2, and 5:</p> <p>The default is Group 1 and 2 selected.</p> <p>Note: <i>If more than one group is selected, the 700wl Series system will not accept any client requests to do Aggressive Mode negotiation.</i></p>

Table 7-1. IPSec configuration settings

Field	Description
ESP Encryption	<p>Select the appropriate algorithms for ESP encryption, or specify None. The 700wl Series system supports the following algorithms:</p> <ul style="list-style-type: none"> • DES • 3DES • AES • Blowfish • CAST • Null <p>The default is DES, 3DES, and AES selected.</p>
ESP Integrity	<p>Select the appropriate algorithms for ESP integrity, or specify None. The 700wl Series system supports the following algorithms:</p> <ul style="list-style-type: none"> • SHA-1 • MD5 • Null <p>The default is SHA-1 and MD5 selected.</p>

- » To save the settings, click **Save**.
- » Clicking the **Reset to Defaults** button resets the Wireless Data Privacy settings to the system defaults. You must **Save** to have these take effect.

IPSec Certificate Configuration

IPSec can use either a shared secret or a a public key infrastructure (PKI) certificate for authentication.

To use certificated-based Internet Key Exchange (IKE) authentication for IPSec, you must request and install a signed local certificate and a root certificate self-signed by the Certification Authority (CA) that signed the local certificate. Once you have installed these certificates, you should 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.

The 700wl Series system does not support chained certificates.

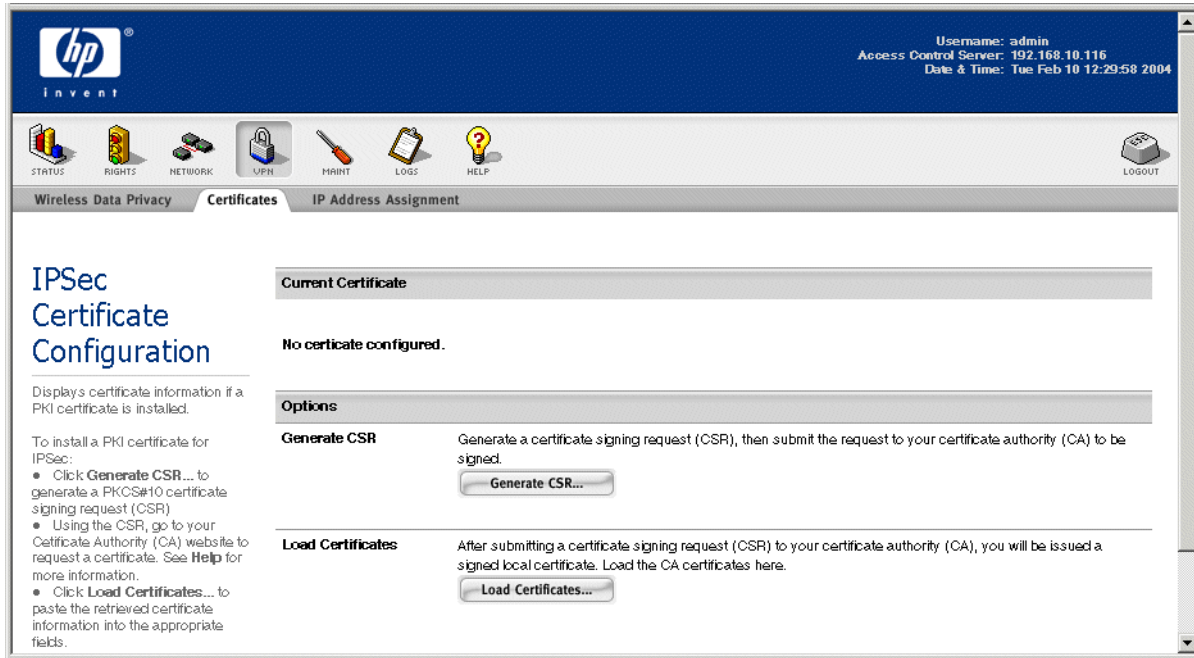
The process for installing a PKI certificate requires that you create a Certificate Signing Request (CSR) through the 700wl Series system Administrative Console embodying information about the HP ProCurve Access Control Server or Integrated Access Manager on which you will install the certificate. You then provide the CSR to a Certification Authority, and then paste the resulting certificates into the 700wl Series system.

To generate and store PKI certificates, do the following:

- Step 1.** Click the **VPN** icon in the Navigation bar at the top of the Administrative Console, then click the **Certificates** tab. This displays the IPSec Certificate Configuration page, as shown in Figure 7-2.

Setting up Wireless Data Privacy

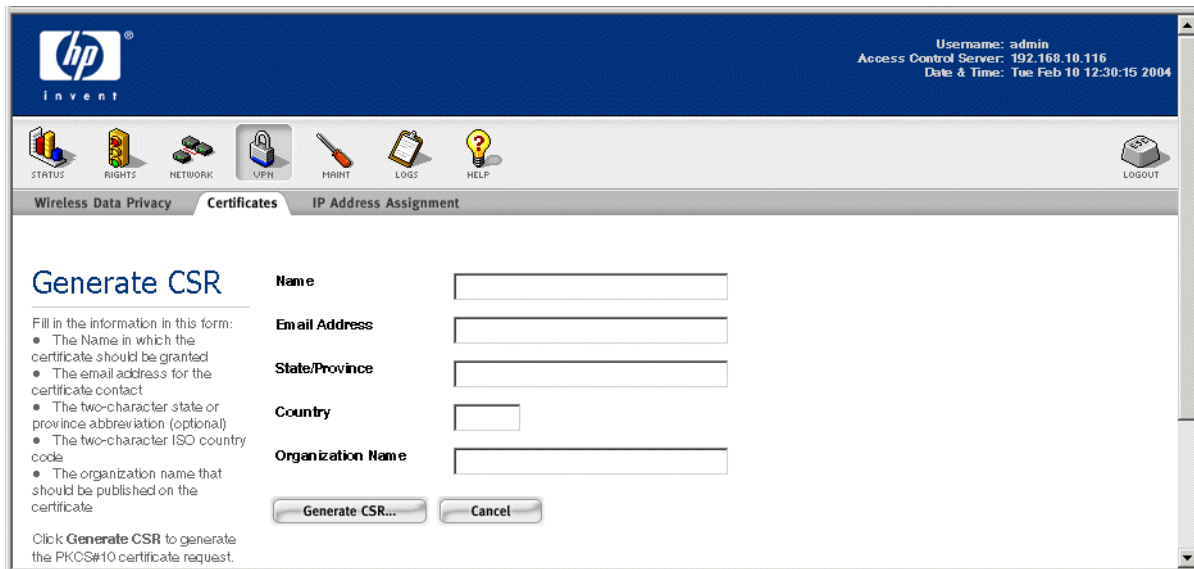
Figure 7-2. The IPsec Certificate Configuration tab



By default the Current Certificate area of the page shows “No certificate configured.” This area will show information about the certificate if one is installed.

Step 2. Click **Generate CSR...** to begin creating a Certificate Signing Request. The Generate CSR page appears, as shown in Figure 7-4.

Figure 7-3. The Generate CSR form



Step 3. Fill in the information in this form:

- Type the name in which the certificate should be granted. This can be an individual name or a title such as "Wireless Admin."
- Type the email address for the certificate contact.
- Type your state or province. This is typically a two-character abbreviation.
- 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>
- Type your organization name. This is the name that will be published on the certificate.

Step 4. Click **Generate CSR** to generate the certificate request.

This produces a PKCS#10 certificate request that you can paste into a CA's certificate request form. Figure 7-4 is an example of a generated request.

Figure 7-4. The Generated CSR request

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. The top navigation bar includes 'Wireless Data Privacy', 'Certificates', and 'IP Address Assignment'. The 'Generate CSR' page is active, showing instructions and a generated CSR request. The CSR request is a long alphanumeric string enclosed in a box, with '-----BEGIN CERTIFICATE REQUEST-----' and '-----END CERTIFICATE REQUEST-----' markers. Below the CSR request is a 'Done' button.

Step 5. Connect to your Certificate Authority web site, 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, for example, 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 Console, and connect to the CA web site from the same system on which you are running the Administrative Console. You cannot request a certificate through the CA's manual request interface. Certificates you receive through that process will not work with the 700wl Series system.

Setting up Wireless Data Privacy

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.

Once you have copied and pasted the CSR, click **Done** to return to the IPsec Certificate Configuration page.

Figure 7-5 shows the enrollment form of a Netscape Certificate Management System with the CSR pasted into the PKCS#10 text area.

Figure 7-5. A Certificate Management System Enrollment form

The screenshot shows the Netscape Certificate Manager interface. The title bar reads "Netscape Certificate Management System" and "Certificate Manager". The main navigation tabs are "Enrollment", "Renewal", "Revocation", and "Retrieval". The "Enrollment" tab is selected. On the left, there is a sidebar with various options: "Browser", "Manual", "Server", "SSL Server", "Registration Manager", "Certificate Manager", "OCSP Responder", "WTLS", "Client", "Server", "Other", "Object Signing (Browser)", "Object Signing (PKCS10)", "CMC", and "Enrollment". The "Enrollment" option is highlighted. The main content area is titled "Server Certificate Enrollment (for Server Administrators)". It contains the following text: "Use this form to submit a request for a server certificate. You must submit a PKCS #10 request. If you have a Netscape server, create a PKCS#10 request by using the Netscape Administration Server instance associated with the server for which you are requesting the certificate. In the Netscape Administration Server forms, choose Encryption, then Request Server Certificate." Below this, it says: "If you are not using a Netscape server, follow the appropriate steps to generate a PKCS #10 request with the server you have." Further down, it states: "After you click the Submit button, your request will be submitted to an issuing agent for approval. You will receive the certificate in email when it has been approved." The "PKCS #10 Request" section has a text area with the following content: "Paste the PKCS #10 request into this text area." followed by a text box containing a long base64-encoded string: "aW5pc3RyYXRvcjEgMCgGCSqGSIB3DQEJARYbd2xhb1h2G1pbk3aXJlbGVzcy1zZW5uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDCviArL51XIjd77I6u21H4/FjdZX+PL/3zj/Grrxb1Y2P7FF1zyXM5DoFwP1Uh5EWI+XzPk+12Y3qRwLBYfjhXAtkq49BHd23UY1V0sO2RD19T1jldqnpojafdr8wGqbe1qdkynG+3xa6zOKj7KfezoH/XyjfVC19bc8zJP8ptZwIDAQABoAAADQYJKoZIhvcNAQEEBQADgYEAcdFCY/XCB4P1X+2FMM7K//U5eVuv5q5kBSimXrOF3wKUxchFO2PMkGWFgsctI8VNjUO3srLvEsn+qPNDUjh7xo+LED/yms4taEYDwRcoppqHLJ3WIPuBb5FQ013Fm2b4dTmt8tjbr7mwv3efW2iIDngm8YpUWund8JikSB+cEuu=" and "-----END CERTIFICATE REQUEST-----". Below the text box is the "Server Administrator Contact Information" section with three input fields: "Name: Bea Goode", "Email: bgoode@wireless-sec.com", and "Phone: 650-512-1212".

Step 7. You may be asked to fill in additional information, such as your contact information. In the example shown in Figure 7-5, 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 root certificate.

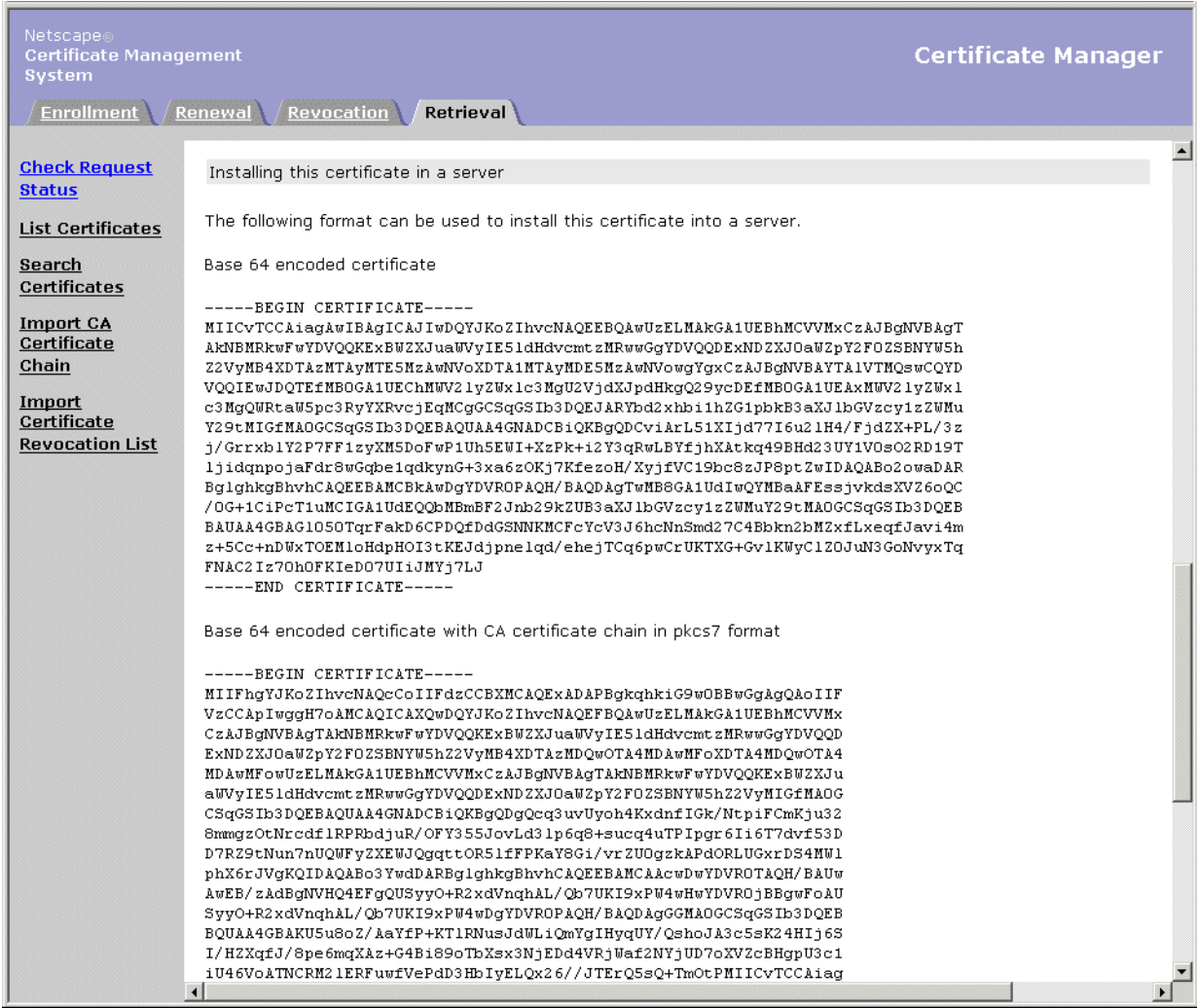
Step 10. On your CA's web site, go to the location where you can retrieve your certificates.

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.

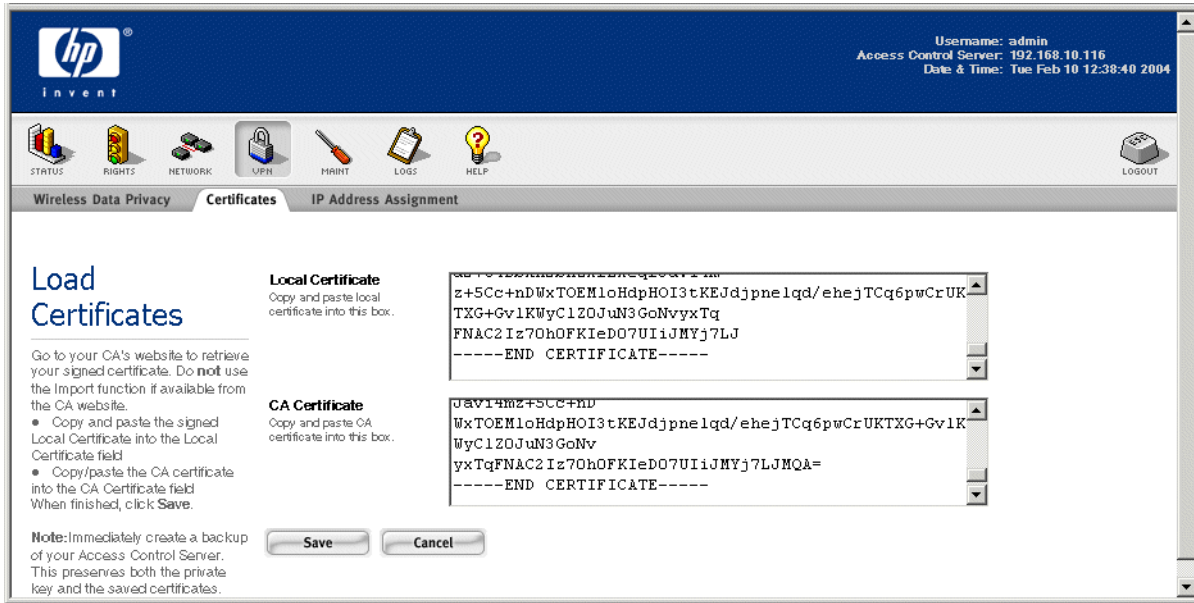
The example in Figure 7-6 shows the portion of the certificate where the information you need to copy is located. Note that the certificates are in the same format as the certificate request you generated. In this example, the local certificate information is in the first block, and the CA certificate is in the second block.

Figure 7-6. A Certificate Management System certificate retrieval page



Step 11. From the IPsec Certificate Configuration page, click **Load Certificates...** This displays the Load Certificates page, as shown in Figure 7-7.

Figure 7-7. The Load Certificates page



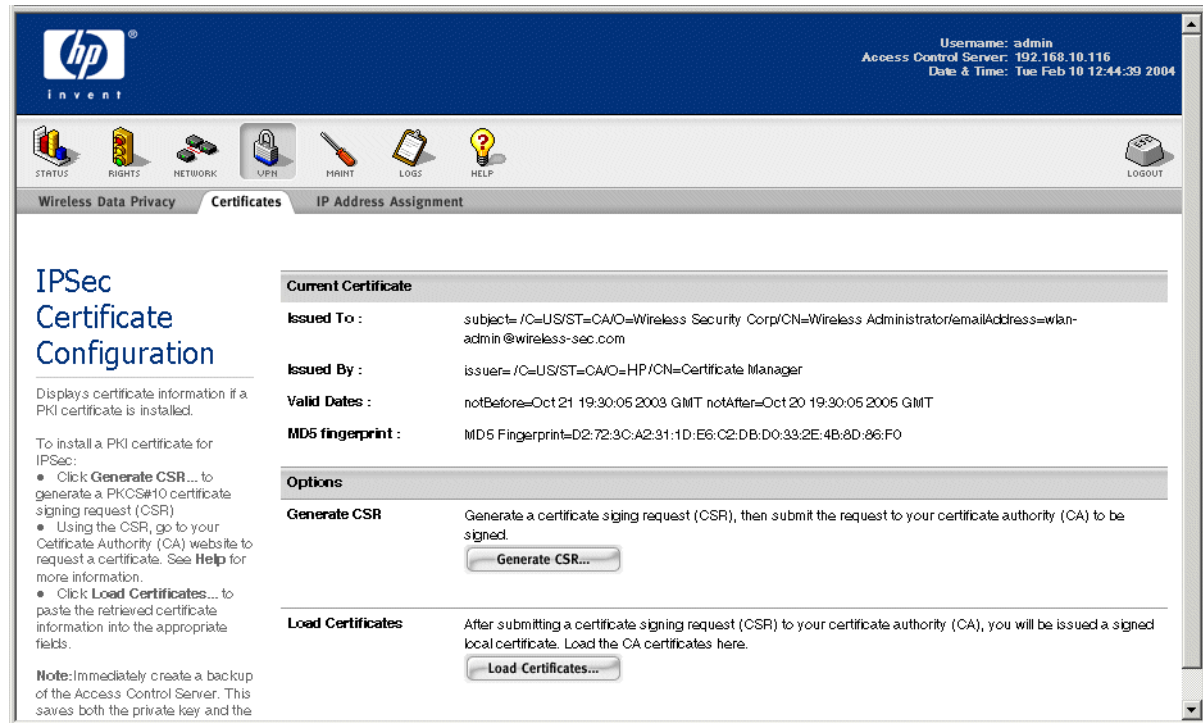
Step 12. Copy and paste the two certificates from your CA's web site into the two fields provided, and click **Save**.

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

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 700wl Series system. You must paste the certificate information into the fields provided in the Load Certificates page in the HP administrative interface.

Figure 7-8 shows the IPsec Certificate Configuration page after a certificate has been installed.

Figure 7-8. The Certificates tab showing an installed certificate



Step 13. Immediately create and save a backup of your system. This saves both the private key and the saved certificates. See “Backing Up and Restoring the System Configuration” on page 8-13 for information on backing up your system.

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.

IP Address Assignment for Tunneling

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.

Note: The same tunneling address assignment method is used by both PPTP/L2TP and IPSEC.

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 a 700wl Series system 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).

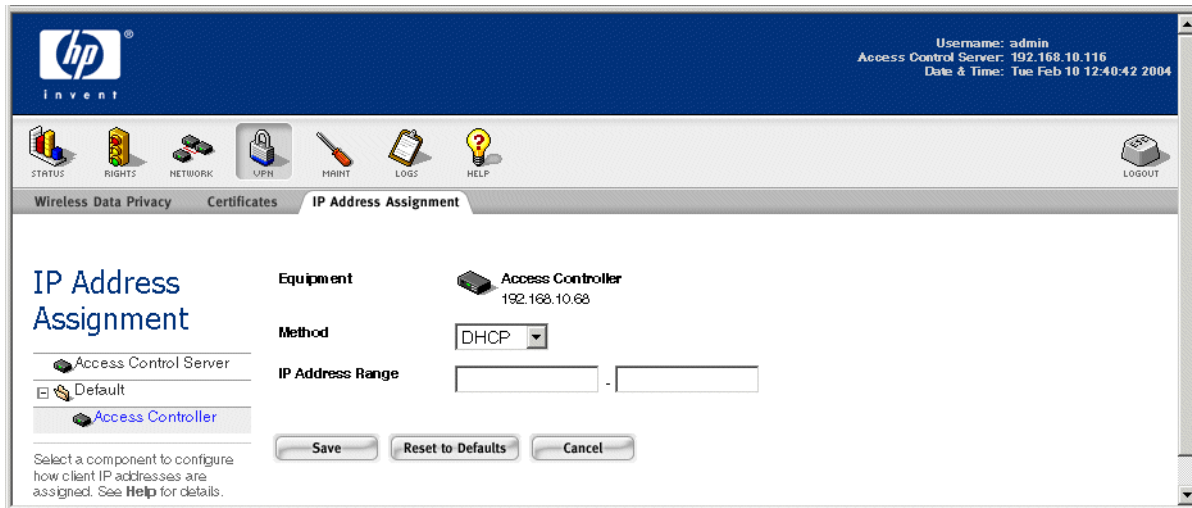
An HP ProCurve Access Controller can be configured to assign this inner-tunnel address in one of two ways: it can either assign an address from a range of addresses pre-specified by the network administrator, or it can request an external DHCP server to assign an address.

Setting up Wireless Data Privacy

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

- » To configure the IP Address assignment method for the tunneling protocols, click the **VPN** icon in the Navigation bar at the top of the Administrative Console, then click the **IP Address Assignment** tab. This displays the IP Address Assignment page, as shown in Figure 7-9.

Figure 7-9. The IP Address Assignment tab



Step 1. In the System Components List, select the Access Controller for which you want to configure IP addressing.

Step 2. On this page, enter values into the fields as described in Table 7-2 below.

The fields under the **IP Address Assignment** tab are as follows:

Table 7-2. IP Address Assignment settings

Field	Description
Method	Select the method you want to use to assign inner-tunnel IP addresses from the drop-down menu <ul style="list-style-type: none">• Select DHCP to assign the address via an external DHCP server• Select Client IP to have the Access Controller assign the address from a range of addresses you provide
IP Address Range	If you selected Client IP , type the beginning and ending addresses of the range you want to use into the fields provided

Step 3. To save the settings, click **Save**.

VPN Tunneling and Network Address Translation

The use of VPN tunneling affects IP addressing and Network Address Translation (NAT). If PPTP or L2TP is enabled Access Policy, 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, even if the Access Policy specifies **Never** for the Network Address Translation setting.

Note: *A side-effect of this behavior is that if encryption is “Allowed but not required” by the Access Policy, and a client connects without using a tunneling protocol, that client will always be NAT’ed upon making a DHCP request. The client will avoid being NAT’ed only if the Access Policy allows static IP addresses, and the client actually uses a static IP address.*

- The inner tunnel address is assigned in accordance with the Access Policy’s NAT setting. However, if Real IP mode is used, the client’s IP address is assigned based on the tunneling configuration specified here—either via the external DHCP service or from a specified address range.

SYSTEM MAINTENANCE

This chapter explains how to perform common administrative tasks including creating, storing, and restoring a back up file, updating system software, and shutting down a 700wl Series system component. It also describes how to reset the 700wl Series system to its factory default settings. This chapter covers the following topics:

Software Setup	8-1
Updating the System Software	8-2
Checking for Upgrade Availability	8-5
Restarting Using the Alternate Version Software	8-12
Backing Up and Restoring the System Configuration	8-13
Restoring From a Backup File	8-16
Shutting Down and Restarting a System Component	8-18

The Maintenance pages provide functions for common administrative tasks including creating, storing, and restoring a back up file, updating system software, and shutting down a 700wl Series system component.

Note: *You must have Network Administrator or Super Administrator access to perform the functions described in this chapter.*

Caution: *Many of the functions discussed in this chapter involve restarting a 700wl Series system component. Restarting an Access Controller in most cases should not log off clients, but restarting an Access Control Server or Integrated Access Manager will log off all clients on all Access Controllers. If possible, you should perform functions that require a system restart during times when few clients are actively connected to your system.*

Software Setup

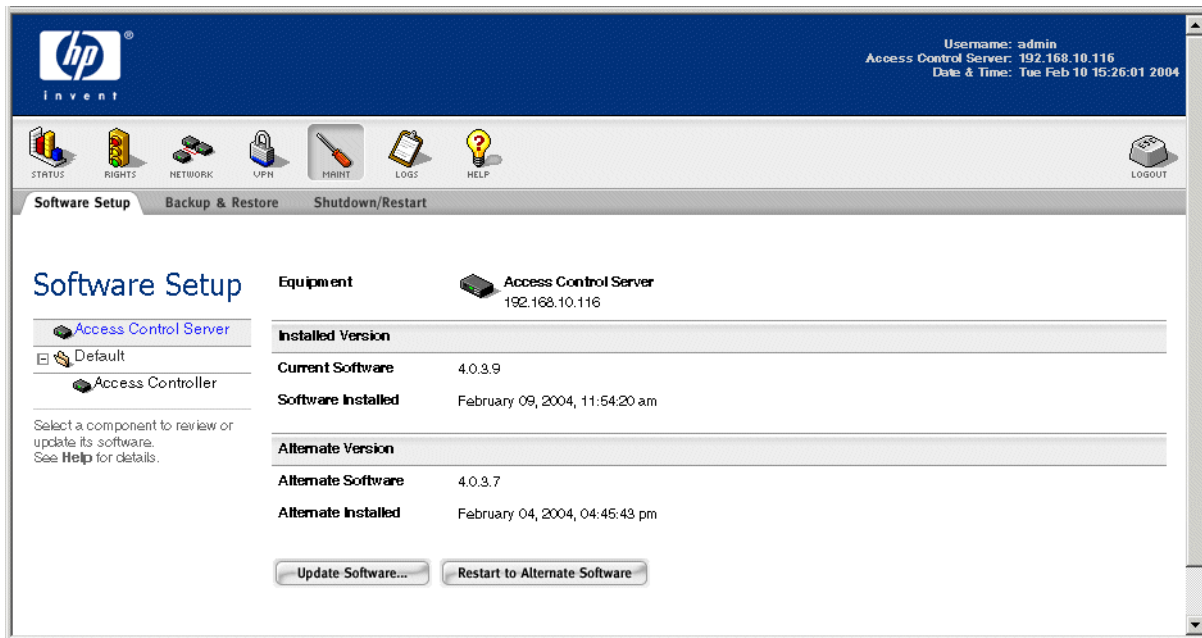
The Software Setup tab of the Maintenance module lets you manage the software running on a 700wl Series system component. A 700wl Series system component maintains two separate software images—the *Installed Version*, which is the version currently running on that unit, and the *Alternate Version*, which is typically the version of the software that was running on the unit prior to the most recent software upgrade.

To manage the system software running on a 700wl Series system component, do the following:

Step 1. Click **MAINT** in the Navigation bar or click the **Software Setup** tab within the Maintenance module.

The Software Setup tab opens—for example, as shown in Figure 8-1.

Figure 8-1. Software Setup page



Step 2. From the System Components list in the left panel, select the component (Access Control Server or Access Controller) for which you want to restart or update the software image.

This page displays information about the software installed in the selected component:

Table 8-1. Software Setup version status display

Field	Description
Installed Version	
Current Software	The version number of the software image currently running in the selected unit.
Software Installed	The date that the current version was installed
Alternate Version	
Alternate Software	The version number of the software image maintained as the alternate version.
Alternate Installed	The date that the alternate version of the software was installed.

From this page you can install a new software image, or restart the selected component using the Alternate Version of the software.

Updating the System Software

To update the software image on a 700wl Series system, you download new system software to the selected component and restart the component to use the new software image.

Note: In order to update flash-based Access Controllers, the update process must 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, and any remote CLI sessions over SSH will be terminated. It is recommended that you update your flash-based Access Controllers during times when system usage is low.

Upgrading the software image is a two step process.

- First, download the software to the selected component. The downloaded software becomes the Alternate Version overwriting the previous Alternate Version.
- Second, restart the component using the Alternate Version just downloaded. You can set this to occur automatically after the download, or you can use the manual restart. Upon restart, the Alternate Version becomes the Current (Installed) version, and the previous Current Version becomes the Alternate Version. This arrangement provides an easy way to revert to the previous software.

When the software image is updated, all the system configuration settings are preserved. The exception to this is the upgrade from software version 3 to software version 4, where some configuration settings, such as the rights configurations, are not preserved.

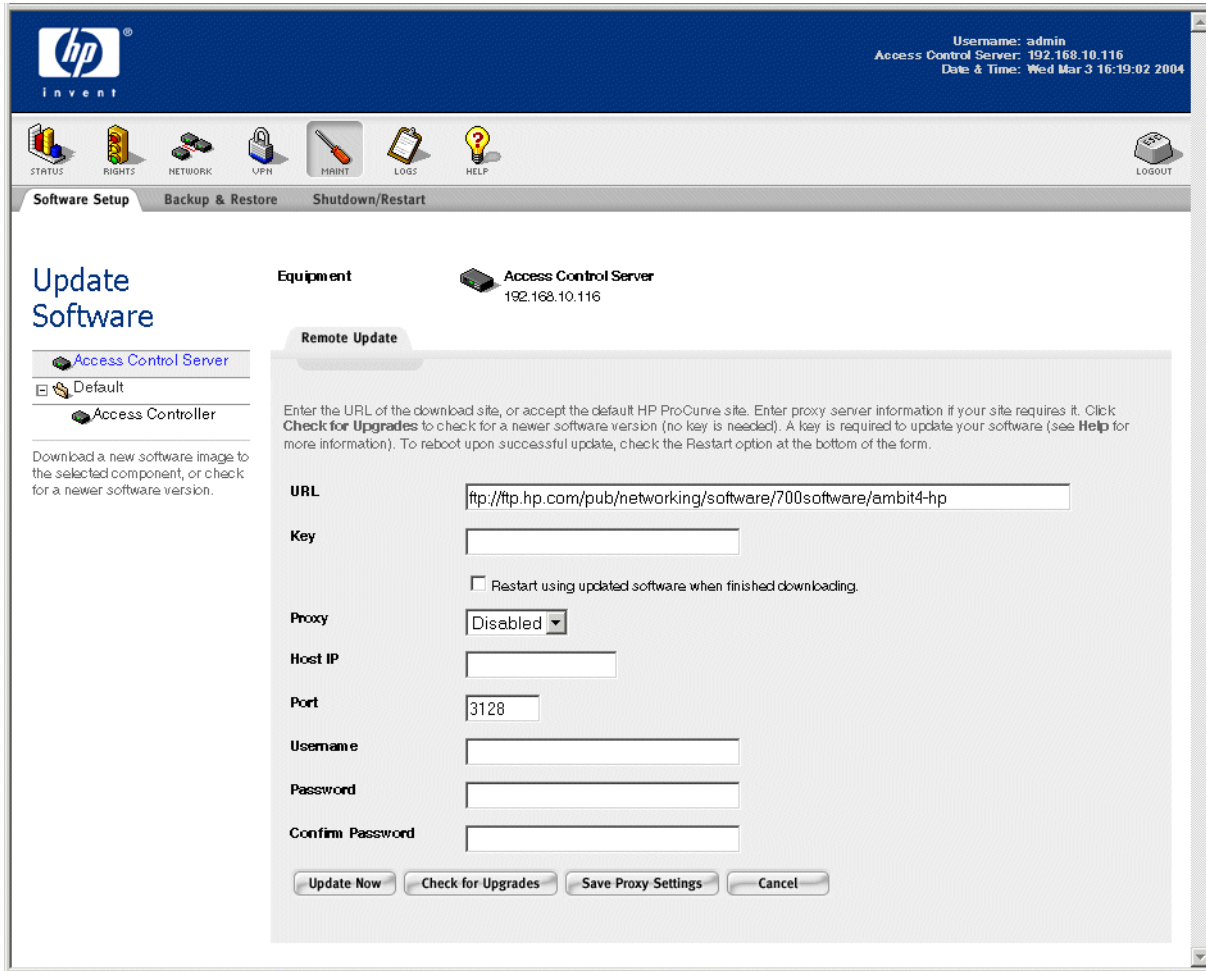
Caution: *Before updating system software, you are strongly advised to create a backup of your current system software. See “Backing Up and Restoring the System Configuration” on page 8-13 for details.*

Step 1. Click **MAINT** in the Navigation bar to display the **Software Setup** tab.

Step 2. Click **Update Software...**

The Update Software page appears with the Remote Update tab displayed, as shown in Figure 8-2.

Figure 8-2. The Update Software page



From the Remote Update page you can initiate a software update from a remote FTP, TFTP, or HTTP server, or just check to see if any updates are available.

Alternately, you may be able to perform an update using a software distribution file placed on a local server. See “Local Update” on page 8-9 for more information on this option, found under the Local Update tab.

Remote Update

The information that is required to update the software image from a remote site is described in Table 8-2.

Table 8-2. Update Software, field/settings descriptions

Field/Option	Description
URL	<p>The URL from which you want to check for software upgrade availability, or download a new version.</p> <p>By default, this field contains the location of an HP ProCurve 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.</p> <p>If you know that a software update is available on another site you may also download from a TFTP or HTTP server. See "Support for Alternate Download Sites" on page 8-8 for more information on alternate download features.</p> <p>The default URL to get the latest software from HP is:</p> <pre>ftp://ftp.hp.com/pub/networking/software/700software/ambit4-hp OR ftp://ftp.hp.com/pub/networking/software/700software/ambit4-am-hp for an Access Controller</pre>
Key	The key is a password that allows you to download and use the 700wl Series system software.
Restart using updated software when finished downloading	Check this to specify that the system should be restarted automatically using the newly-downloaded software. The default is not to do an automatic restart.
Proxy	Select Enabled to go through a proxy server, as configured in the fields that follow. A proxy service enables you to download the new image through an enterprise firewall. Select Disabled if you do not use a proxy service.
Host IP	The IP address of the proxy server
Port	The port number of the proxy service. The default is 3128.
Username	The username required for proxy access
Password	The password required for access
Confirm Password	The password, entered a second time for confirmation

If you use a proxy service, you can save the proxy server settings so you do not need to enter them every time to do an upgrade.

» To save your proxy settings, click **Save Proxy Settings**.

Checking for Upgrade Availability

To check for the availability of an upgrade on the HP ProCurve download site, do the following:

Step 1. Fill in the fields as appropriate. If you want to check for upgrades from the default HP ProCurve download FTP site, you can leave all fields as they are.

You do not need to enter a key to check for upgrade availability. (However, entering the key enables you to download the upgrade immediately if an upgrade is available.)

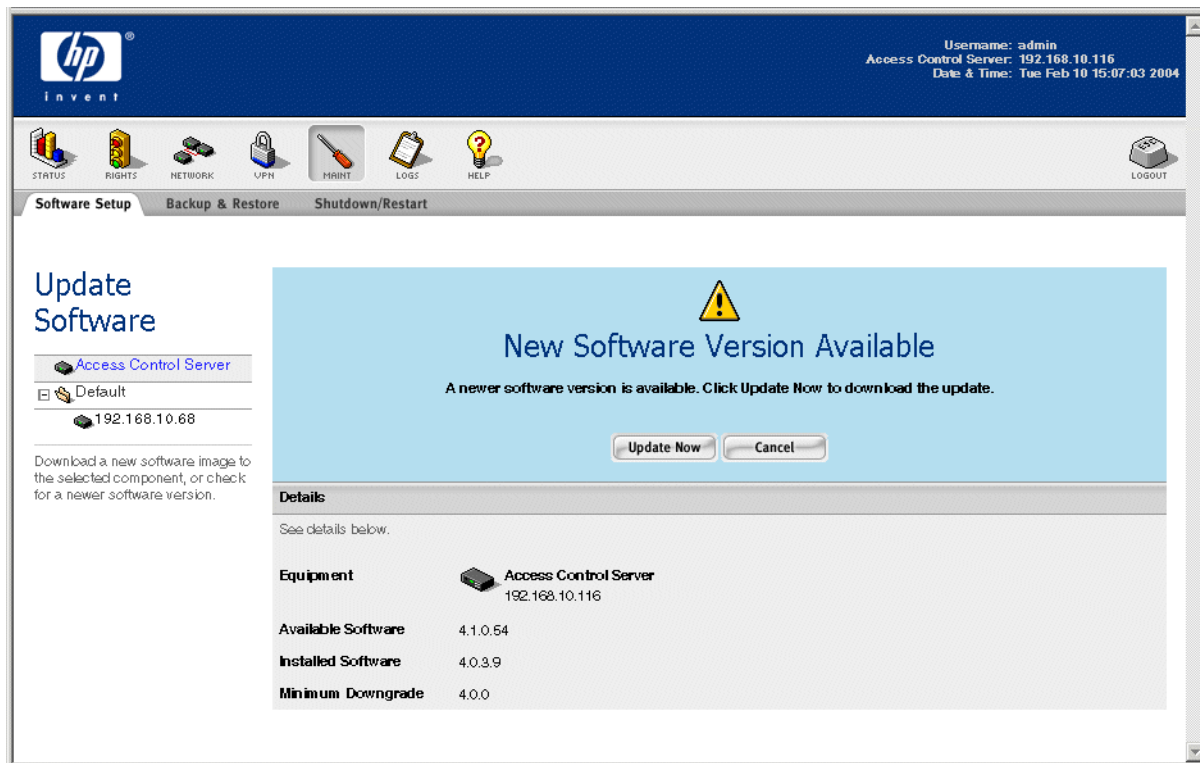
System Maintenance

If you want to check for upgrades on an alternate download site, you must enter the appropriate URL.

Step 2. Click **Check for Upgrades**.

This function checks the software version available on the download site against the software version currently installed in the component you have selected. A Confirm Software Update page opens, showing that the current version is up to date or that there is an update available. Figure 8-3 shows an example of this page.

Figure 8-3. Results of a check for upgrade availability



Step 3. If a new upgrade is available, you can choose to upgrade immediately, as long as you included the upgrade key on the previous page, or click **Cancel** to return to the previous page.

Downloading an Upgrade

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

Step 1. Fill in the appropriate fields as described in Table 8-1.

If you use a proxy server, you can save the settings so you do not have to reenter them whenever you do an upgrade—click **Save Proxy Settings**.

Step 2. Click **Update Now**.

A download key is required for this operation.

Step 3. You will be asked to confirm the upgrade, and, if appropriate, that you want to automatically restart upon a successful download.

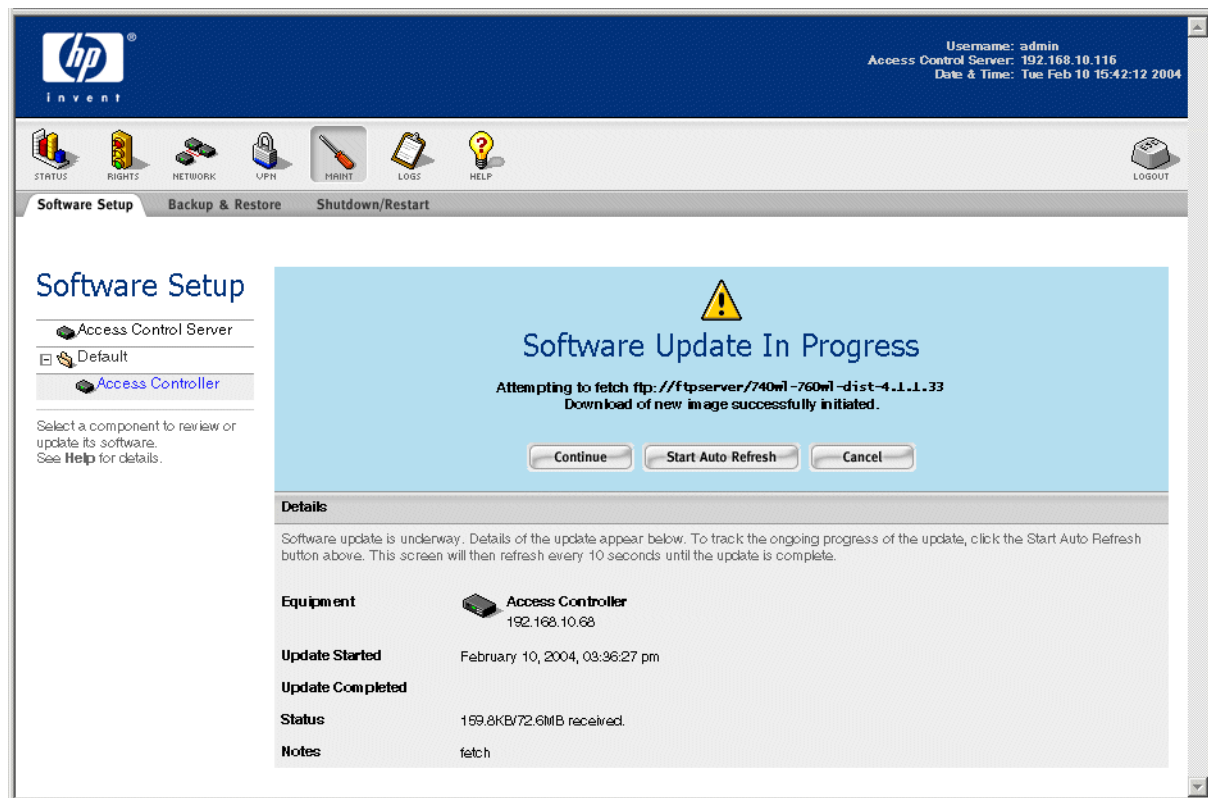
Select **Continue** to proceed with the upgrade, or **Cancel** to return to the previous page without proceeding.

Note: If your currently installed software is significantly older than the new version you are downloading, it may not be possible to revert to your old (Alternate) image without doing a factory reset, which restores the unit to its default settings. If this is the case, a warning is displayed advising you to make a backup of the system before proceeding with the upgrade. If you save a backup, you will then be able to restore your configuration if a downgrade to your older version becomes necessary.

Caution: If you upgrade or downgrade a unit to a software version that is significantly different from the version running on the other units in your system, it is possible that the unit may no longer be able to communicate with other units on your system. See the release notes for the affected software versions for possible information on compatibility across the 700wl Series system between software versions. In particular, units running software version 4.0 or later cannot communicate with units running software version 3.1 or earlier.

Figure 8-4 shows the Update Progress page that normally appears immediately after you have confirmed the download. If you want a continuous status update, click **Start Auto Refresh**. Otherwise, the status is not updated.

Figure 8-4. Software Update Progress Display



System Maintenance

If you enable Auto Refresh, the status page refreshes approximately every 15 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 restart, the status message also displays **Initiating reboot** and the restart operation starts.

Step 4. If you did not specify an automatic restart, you can return to the Update Software page as soon as the download has completed to perform another upgrade on a different unit.

The Software Setup tab displays both the installed software version as well as an alternate version, which should be the newly-downloaded version. You must then restart to the alternate version to complete the update of the software.

Step 5. To initiate a restart of the unit, return to the Software Setup tab and select **Restart to Alternate Software.**

When the system has restarted, the newly-downloaded version should appear as the Installed Version under the Software Setup tab. The previously installed version should appear as the Alternate Version.

Caution: *Restarting an Access Control Server or Integrated Access Manager will log off all clients on all Access Controllers. If possible, you should perform an upgrade and restart during a time when clients are not actively connected.*

Support for Alternate Download Sites

By default the download URL specifies the location of an HP ProCurve FTP server site where the most recent upgrade images are stored. If for any reason you cannot or do not wish to download software images from the HP ProCurve download FTP site, it is possible to obtain the software images and install them on your own FTP, TFTP, or HTTP site.

Note: *To download the software image to a local FTP, HTTP, or TFTP server, please go to www.hp.com/go/hpprocurve.*

If you know that the download images are stored on a different server, you can enter your URL in any one of these URL formats:

- `<protocol>://<host>/<update_file>`
- `<protocol>://<username>[:<password>]@<host>/<update_file>`

where the variables in those formats can be as follows:

Variable	Value
<code>protocol</code>	FTP, HTTP, or TFTP
<code>host</code>	IP address or a server hostname <code>host</code> can include a port— <code>hostname:port</code> —following the host name and separated by a colon
<code>username[:password]</code>	Username and password with access to the remote site, if required

Variable	Value
<code>update_file</code>	<p>Filename (including the path) of the software image</p> <p>Please contact HP ProCurve Technical Support for information on the current downloadable image.</p> <p>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.</p>

For example:

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/ambit4
```

This accesses the FTP server as user "jane" with password "secret" and downloads the image from the full path "/users/ftp/ambit4"

Local Update

The Local Update option allows you to update the software in your 700wl Series system units from a distribution file stored on your Access Control Server or Integrated Access Manager, rather than from a remote system. This means that your 700wl Series system units do not need external (Internet) access in order to obtain the update. (The Remote Update option assumes that the 700wl Series system unit being updated can access the HP ProCurve technical support web site to download the update.)

The distribution file must initially be downloaded from the HP technical support web site, but you can download it to any local system—it is not downloaded directly to a 700wl Series system unit. Once the distribution file is stored on a local system, you upload it from the local system into the 700wl Series system Access Control Server or Integrated Access Manager. Software updates of your 700wl Series systems are then performed using the distribution file saved on the Access Control Server or Integrated Access Manager. You can store up to four distribution files on a 700wl Series Access Control Server or Integrated Access Manager.

Obtaining the Software Distribution File

To download a software distribution file from the HP ProCurve Technical Support web site and upload it onto your Access Control Server or Integrated Access Manager, do the following:

Step 1. Download the distribution file from the HP technical support web site to a local system.

Log onto the HP FTP site using anonymous FTP in Passive mode. You will not be able to do a directory listing.

The files to download are:

ambit4.vdist-hp for an Access Control Server or Integrated Access Manager.

ambit4.vdist-hp-am for an Access Controller.

Assuming you plan to update both your Access Control Server and one or more Access Controllers, you need to download both files.

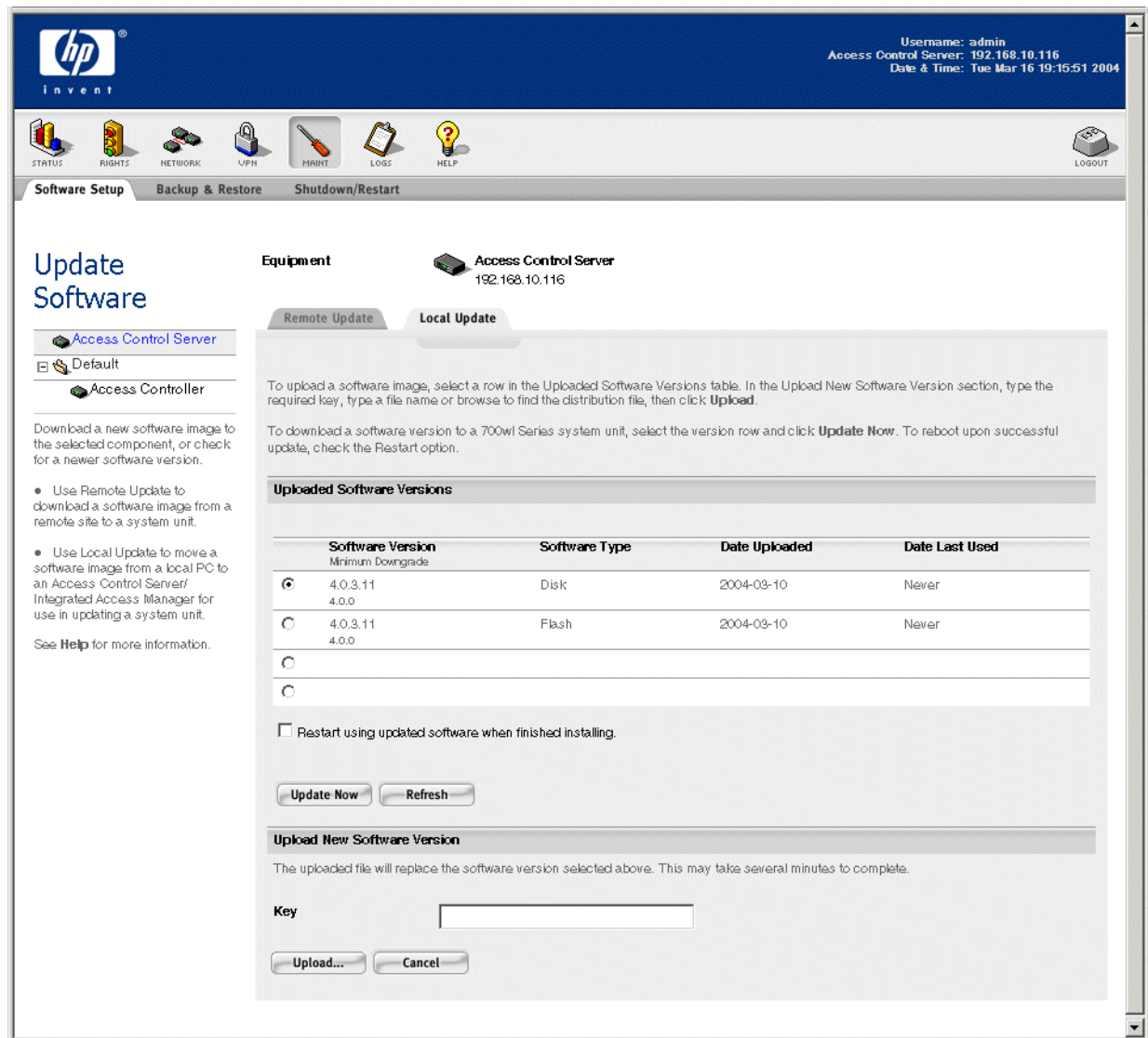
System Maintenance

Step 2. In the 700wl Series system Administrative Console, under Maintenance/Software Update, select the Local Update tab to display the Local Update page, as shown in [Figure 8-5](#).

Table 8-3. Update Software, field/settings descriptions

Field/Column/Option	Description
Uploaded Software Versions	This table shows up to four software versions kept on the Access Control Server or Integrated Access Manager, available for download to any of the system components connected to the Access Control Server or Integrated Access Manager.
Software Version/ Minimum Downgrade	The software version number of this software image. If this version is used as the current running software version in an HP ProCurve system, this is the oldest version to which you can downgrade without a reset to factory defaults being required.
Software Type	Flash indicates that this software version runs on a flash-based Access Controller.
Date Uploaded/ File Name	The date this software version was uploaded The name of the file that was uploaded.
Date Last Used	The most recent date that this version was downloaded to a 700wl Series system.
Restart using updated software when finished installing	Check this to specify that the system should be restarted automatically using the newly-downloaded software. The default is not to do an automatic reboot.
Upload New Software Version	
Key	The key is a password that allows you to upload and use the 700wl Series system software.
Distribution file	The path and filename on a local system where a copy of the HP ProCurve software distribution file is located.

Figure 8-5. The Local Update Tab of the Update Software Function



Step 3. In the **Uploaded Software Versions** table, select the row where you want the new uploaded version to be placed. If there is already a software image in that row, it will be replaced by the new image you upload.

Step 4. In the lower part of the window under the **Upload New Software Version** heading, type the appropriate keyword. The key is a password that allows you to upload and use the 700w1 Series system software. **An upload key is required for this operation.**

You can obtain a key from HP ProCurve by accessing the secure web page on the Technical Support web site at <http://www.hp.com/go/hpprocurve>. See the online help for the Update Software page for more information.

Step 5. Click **Upload...**

This displays a popup window where you specify the distribution file name.

System Maintenance

Step 6. In the **.vdist File** field, type the full path and name of the distribution file you downloaded, or click **Browse** to locate the proper directory and file name.

Note: You can save the vdist files under different names, if you want. They do not need to have a .vdist extension.

Step 7. Click **Upload Image** to upload the software image to the Access Control Server or Integrated Access Manager.

Note: Even if you select an Access Controller in the System Components list in the left panel, the upload will still be done to the Access Control Server.

When the upload is complete, the new software image appears in the Uploaded Software Versions table in the row you selected.

Note: The upload of a flash-AC version is relatively quick; the upload of a full (Access Control Server or Integrated Access Manager) version takes somewhat longer. The cursor will change to include an hourglass icon while the upload is in progress.

Updating a System Component from a Local Software Version

Once you have uploaded one or more software versions to your Access Control Server or Integrated Access Manager, you can update any of your system components using one of those versions.

Step 1. In the System Components list, select the 700wl Series unit you want to update.

Step 2. Select the software version you want to use to update the selected unit.

Step 3. If you want to restart the selected unit immediately upon completion of the download, check the **Restart using updated software when finished installing** option.

If you do not check this option, you can restart the unit later using the Restart to Alternate Software option.

Step 4. Click **Update Now** to start the download. Because a key was required to upload the software to the Access Control Server, you do not need to enter a key to download to a system component.

Restarting Using the Alternate Version Software

Each 700wl Series system component maintains two versions of the system software, the Installed Version, which is the version currently running on that component, and the Alternate Version, which is typically the version of the software that was running on the system prior to the most recent software upgrade.

The Software Setup tab under the Maintenance module displays the version numbers of both the Installed and Alternate versions. From the Software Setup tab you can restart the Access Control Server or an Access Controller using the alternate software version on that system. You might choose to do this in the following situations:

- You downloaded a new software version, which automatically became the Alternate Version, and did not elect to do an automatic restart
- You want to return to the previously-installed version of the software

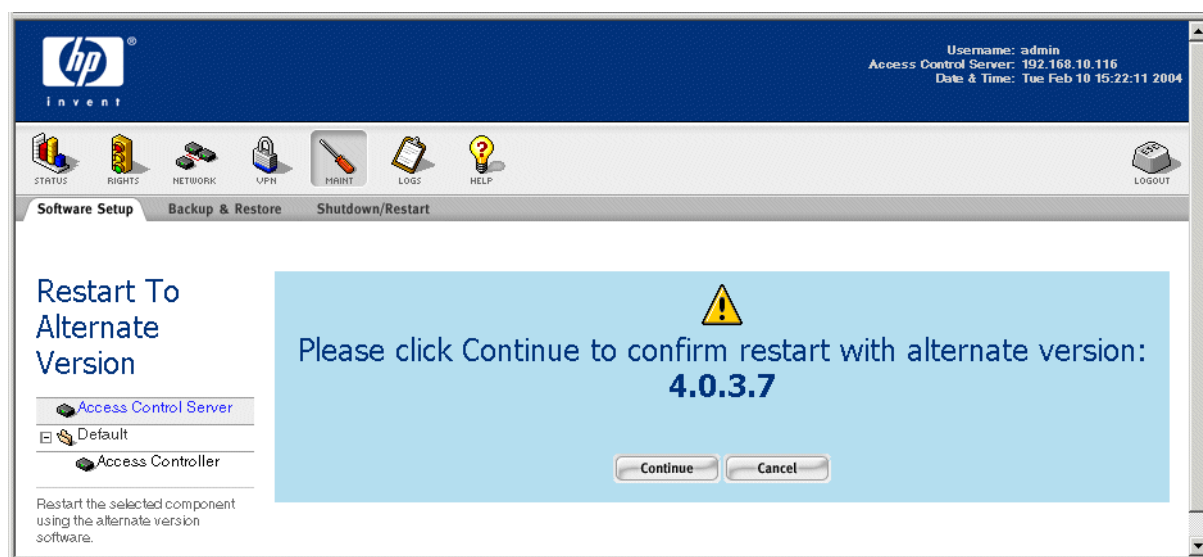
Caution: Restarting an Access Control Server or Integrated Access Manager will log off all clients on all Access Controllers. If possible, you should restart your system during a time when few clients are actively connected to the system.

- » To restart your system using the Alternate software version, click **Restart to Alternate** under the Software Setup tab.

A confirmation/warning page appears. Depending on the relation of the Alternate Version to the currently installed version, a number of possible warnings may appear.

Figure 8-6 is an example of one such warning.

Figure 8-6. Restarting using an older Alternate Version (version downgrade)



Backing Up and Restoring the System Configuration

You should create backup files of your 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" on page 8-2, or if you are restoring to factory defaults, as described in "Resetting to Factory Default Settings" on page 8-21.

Note: The Backup function performed from your Access Control Server backs up the configuration for your entire 700wl Series system, including all Access Controllers associated with the Access Control Server.

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

Creating and saving a backup image is a two-step process:

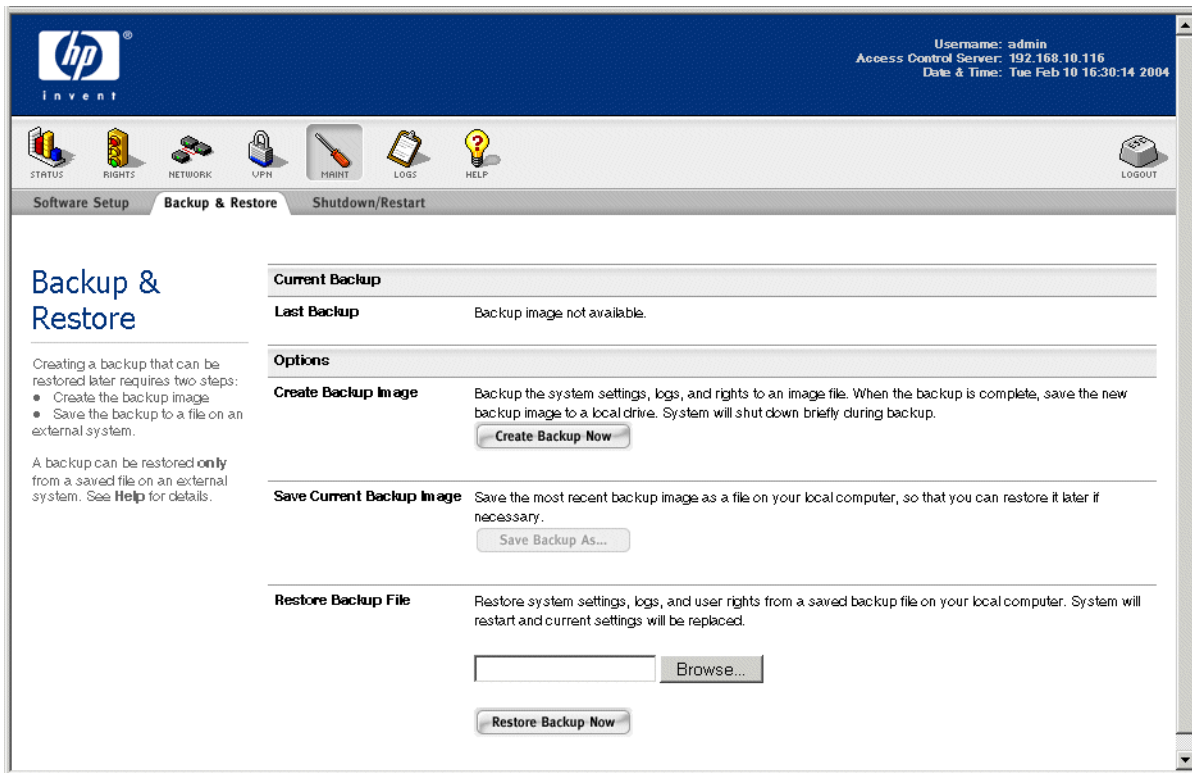
- First, create the backup image. This image is created on the 700wl Series system itself, and overwrites the previously created backup image.
- Second, save the backup image to a file on your local system. This is the file you can use if you ever need to restore your backup configuration.

System Maintenance

Note: You cannot restore from the internal backup image. You can only restore from an external file. Therefore, you **must** save the backup image to a file.

- » To back up a system configuration, click the **Backup & Restore** tab under the **Maintenance** button. The Backup & Restore page appears, as shown in Figure 8-7.

Figure 8-7. The Backup & Restore tab



The Backup & Restore page displays the status of any backups created on the component you have selected, as well as options to create or restore a backup.

The **Last Backup** field displays the date and time that the current backup image (residing in the unit) was created, if any.

If a backup image exists, you can save it to a file, if you have not done so previously. When you create a new backup image, it will overwrite the previous image. If no image exists, the **Save Backup As...** button will not be available.

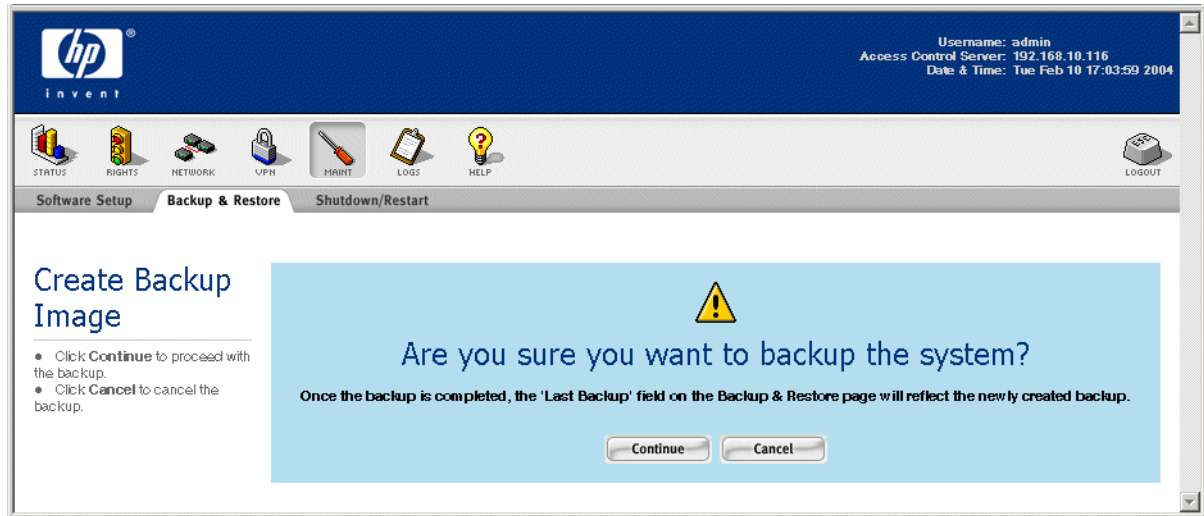
Creating the Backup Image

To create the backup image, do the following:

Step 1. Click **Create Backup Now**.

A confirmation page appears, as shown in Figure 8-8.

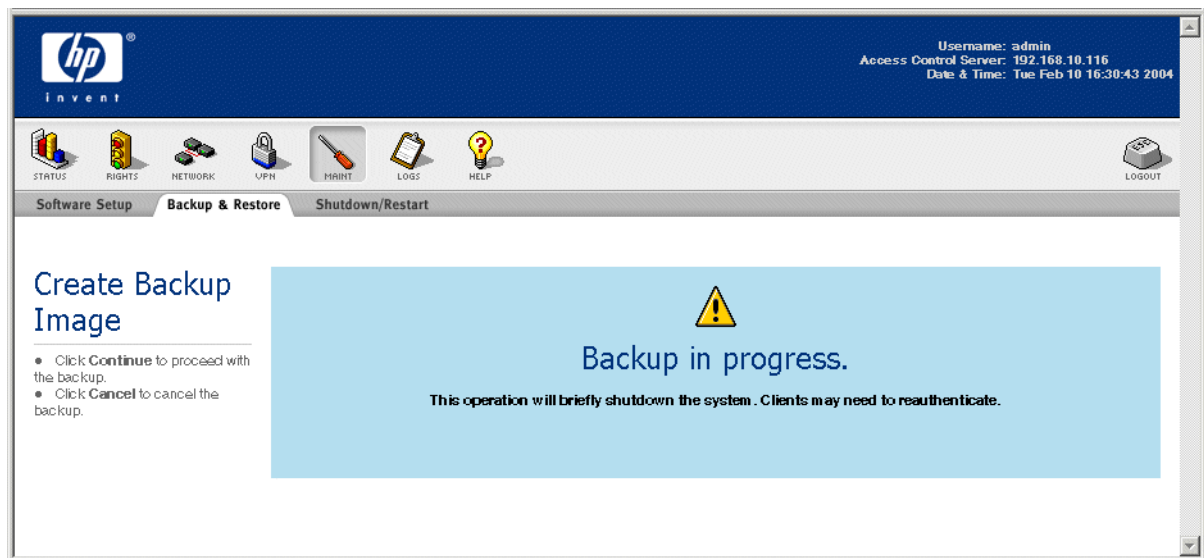
Figure 8-8. Backup Confirmation



Click **Continue** to proceed, or **Cancel** to return to the Backup & Restore page without creating the backup image.

While the backup is in progress, an information page, as shown in Figure 8-9, is displayed.

Figure 8-9. Backup In Progress

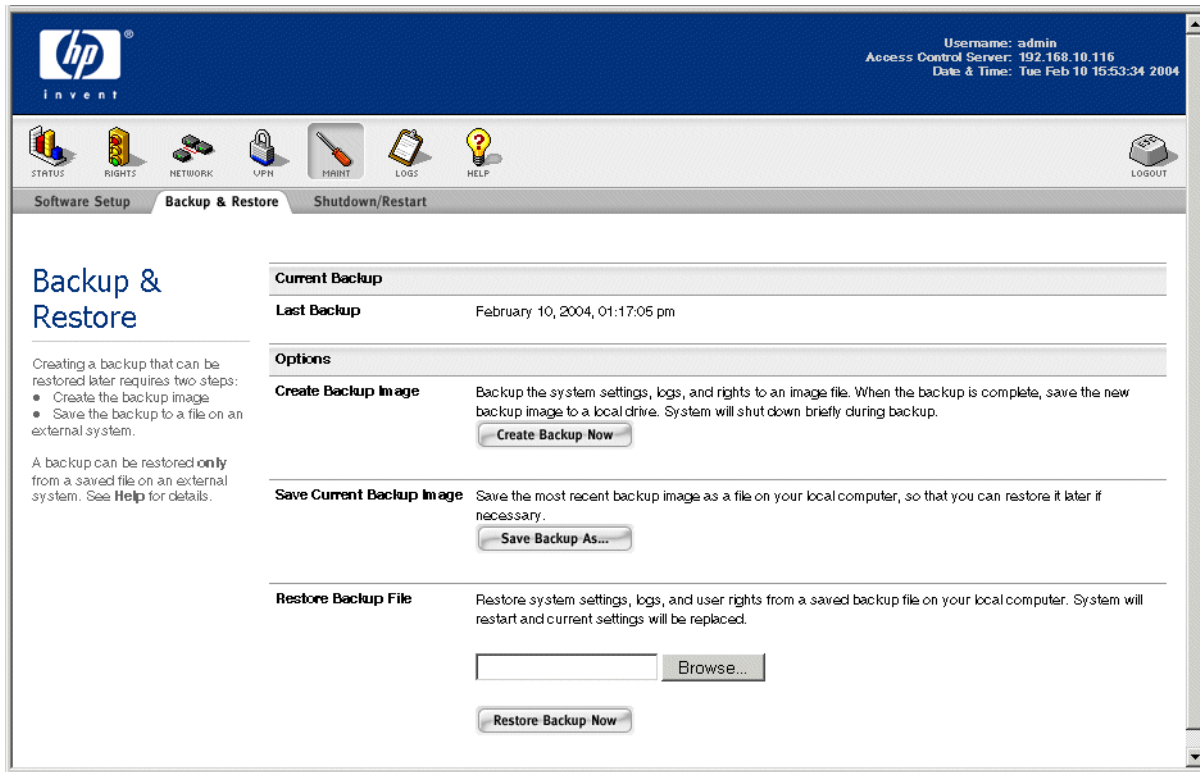


Step 2. When the backup has completed, another informational page appears, telling you the process is complete. This export image will replace the previous export image, if one existed.

Saving the Backup as a File

If the backup image is created successfully, the **Last Backup** field reflects the new backup, and the **Save Backup As...** button becomes available, as shown in Figure 8-10.

Figure 8-10. Backup & Restore page after a successful backup



» To save the backup to a file, click **Save Backup As....**

This initiates the File Download process on your local system. This typically involves a series of dialogs presented by your local system software, where you can select a location to store the file and enter a file name. By default, the backup image file is named “hp” concatenated with the date (-YYYY-MM-DD). You can use this default or rename it.

The exact form of the file download process will depend on the operating system or browser you are using.

Restoring From a Backup File

Note: Restoring an image automatically restarts the system when the file restore is complete. When you restore an Access Control Server or Integrated Access Manager, all clients on all Access Controllers active at the time of the restore will be logged off and will need to reauthenticate.

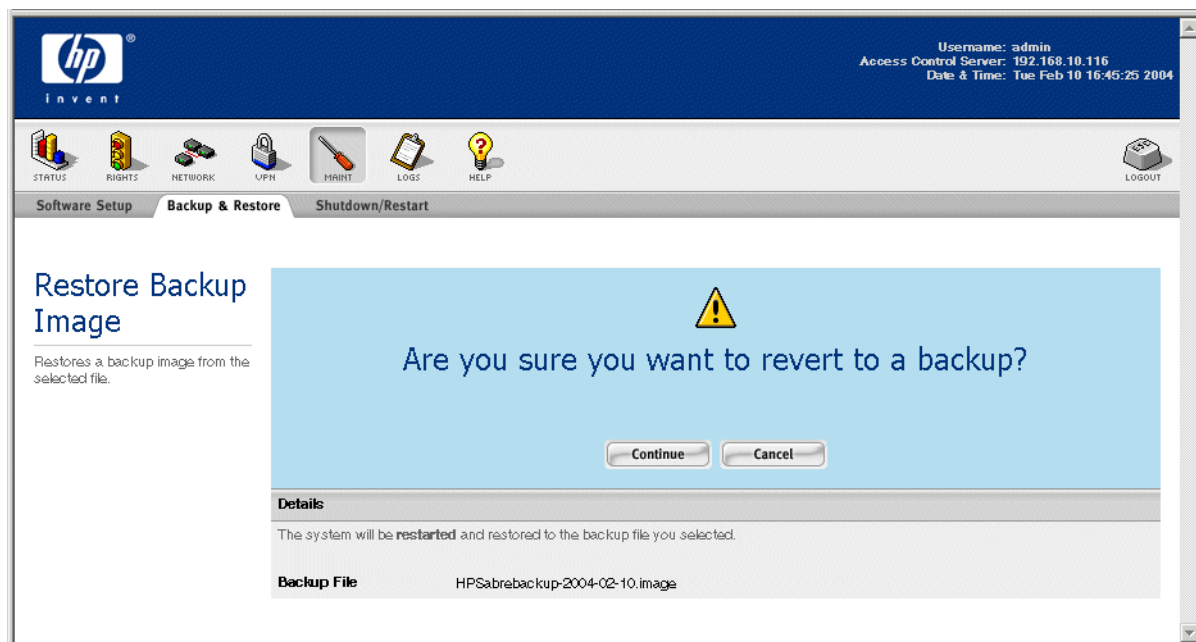
To restore a saved backup from a file, do the following:

Step 1. On the Backup & Restore tab of the Maintenance pages, enter the location of the saved backup file in the field provided, or use the **Browse** feature to locate the file you want to restore (see Figure 8-10 on page 8-16).

Step 2. Click **Restore Backup Now**.

A confirmation page appears, as shown in Figure 8-11, and displays the file you have selected as the backup source.

Figure 8-11. Restore In Progress Confirmation



Step 3. To proceed with the restore, click **Continue**.

As part of the restore operation, the system is restarted. You will be required to log in again as administrator.

Transferring a Backup to a Different System

There may be situations where you want to transfer the configuration from one Access Control Server to another, such as to use the original configuration as the starting point for additional configuration changes you want to verify in a test-bed environment, or to replicate a configuration for installation on a different part of your network.

If you create and save a backup on one system, and then restore it to a different system, the restore reconfigures the new system to exactly match the original (backed-up) system's configuration, including its network configuration, with two exceptions:

- The uplink port will **not** be changed on the new (restored to) unit, but will remain as configured. This is to avoid accidentally changing an uplink port into 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.

- If the new (restored to) unit is a 700w1 Series system, the port power settings will also **not** be changed on the new system, but will remain as configured. This is to avoid accidentally enabling power on a port to which a non-power-capable device is connected, or changing the polarity (from +48VDC to -48VDC) on a port.

Warning: DO NOT restore a backup to a duplicate Access Control Server that is connected to the same network as the original Access Control Server. Restoring a backup will restore the original Access Control Server's IP address (if a static IP address was configured) and the shared secret. This can result in the second Access Control Server taking control of the Access Controllers on the network away from the original Access Control Server. Disconnect the duplicate Access Control Server from the network before restoring the backup, and change its IP address (and shared secret, if appropriate) before reconnecting it to the network.

Shutting Down and Restarting a System Component

Caution: Restarting an Access Control Server or Integrated Access Manager will log off all clients on all Access Controllers. Therefore, if possible you should perform these functions during times when few clients are actively connected to the system.

There are several ways to shut down and restart a 700wl Series system component:

- Through the Administrative Console, via the Shutdown/Restart tab in the Maintenance module
- From the Command Line Interface (see [Appendix A, “Command Line Interface”](#) for instructions)
- From the system display panel of the unit itself (see the *700wl Series system Installation and Getting Started Guide* for your equipment for instructions on using the system display panel.

Shutting down and restarting using the Administrative Console is the recommended procedure.

Shutting down by simply powering off the unit using the chassis power button is NOT recommended, as this may result in corruption of the unit's configuration information, including the status of any clients connected to the system when the shutdown occurred.

Caution: You should backup your system configuration and save it to an external file before you shutdown, restart or reset a system component.

The Shutdown/Restart tab provides several options for shutting down and restarting a system:

- You can perform a system restart, which will shutdown and restart the system. This option does not power down the hardware, and it always restarts the Installed version of the software.
- You can shutdown the hardware, powering off the unit. After a complete shutdown, you can restart the unit from the front panel power switch. (See the *700wl Series system Installation and Getting Started Guide* for your equipment for information about the controls on your unit.)
- You can reset the unit to its factory default configuration. This operation does not power down the hardware, but clears the configuration database and restarts the unit.

To access the shutdown and restart options, do the following:

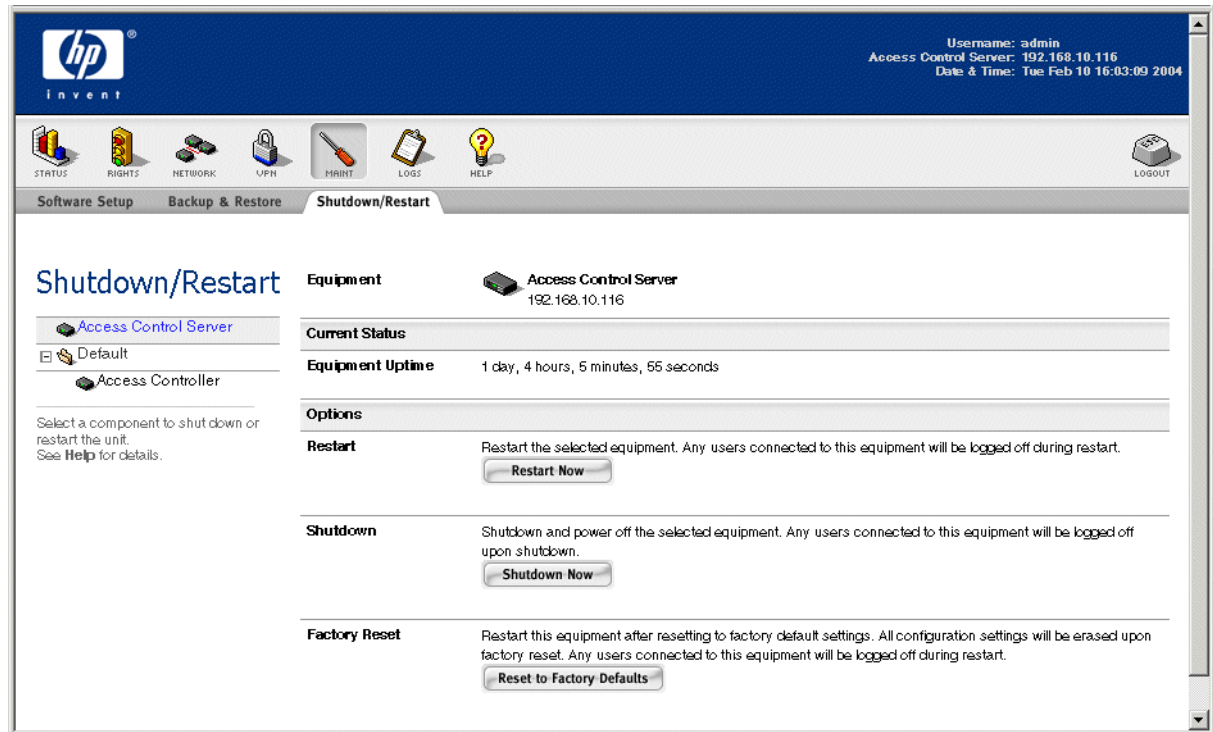
Step 1. From within the Maintenance module, click the **Shutdown/Restart** tab.

The Shutdown/Restart page appears, as shown in Figure 8-12.

Step 2. Select the component you want to shut down or restart from the System Components List at the left of the page.

The Shutdown/Restart page displays the system uptime for the component you have selected, as well as buttons to initiate a shutdown, restart, or reset to defaults action.

Figure 8-12. The Shutdown/Restart tab



Restarting a System Component

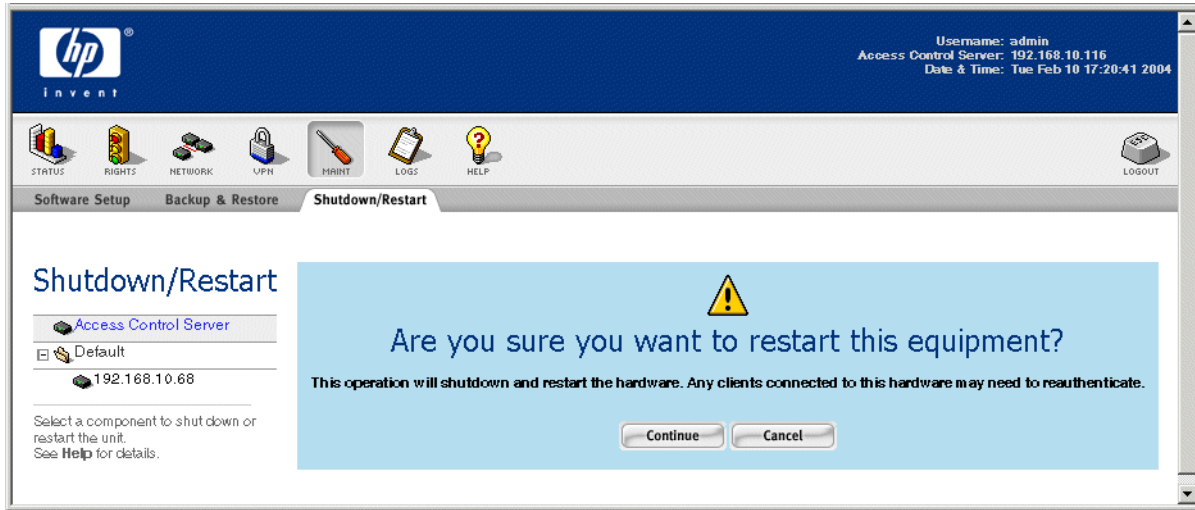
Restarting a component will briefly shutdown the unit, then restart it using the Installed Version software image. This action does not power off the unit.

To restart a selected system component:

- Step 1.** Select the unit you want to restart from the System Components List.
- Step 2.** Click **Restart Now**.

A confirmation page appears, as shown in Figure 8-13.

Figure 8-13. Restart Confirmation



Step 3. To proceed with the restart, click **Continue**.

To cancel the restart, click **Cancel**.

Shutting Down a System Component

Shutting down a system component shuts down and powers off the selected unit.

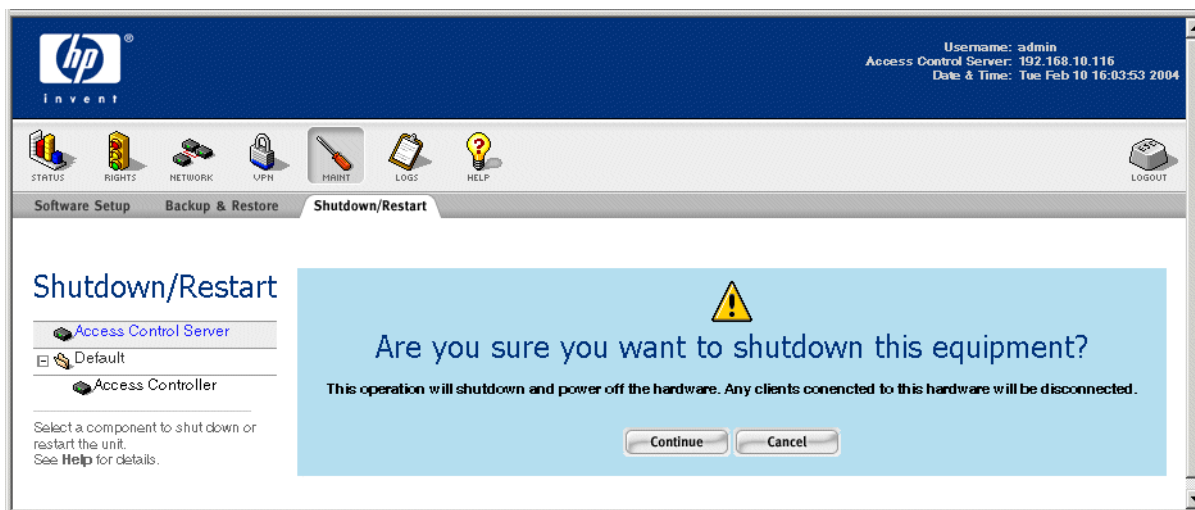
To shut down and power off a system component:

Step 1. Select the unit you want to shut down from the System Components List.

Step 2. Click **Shutdown Now**.

A confirmation page appears, as shown in Figure 8-14.

Figure 8-14. Shutdown Confirmation



Step 3. To proceed with the shutdown, click **Continue**.

To cancel the shutdown, click **Cancel**.

Resetting to Factory Default Settings

Resetting a system to its factory defaults will clear the configuration database, reset all options to the factory default settings, and restart the unit.

Warning: *If you have reconfigured the uplink on this component to use a port other than the default uplink port (such as the gigabit fiber port on an option card) you are strongly advised to remove the unit from the network and do the reset operation using the serial console and CLI.*

A factory reset operation resets the uplink to the default uplink port, and your reconfigured uplink port reverts to a downlink port. This can have adverse effects on your network. You must use the serial console interface and CLI to reconfigure the uplink port.

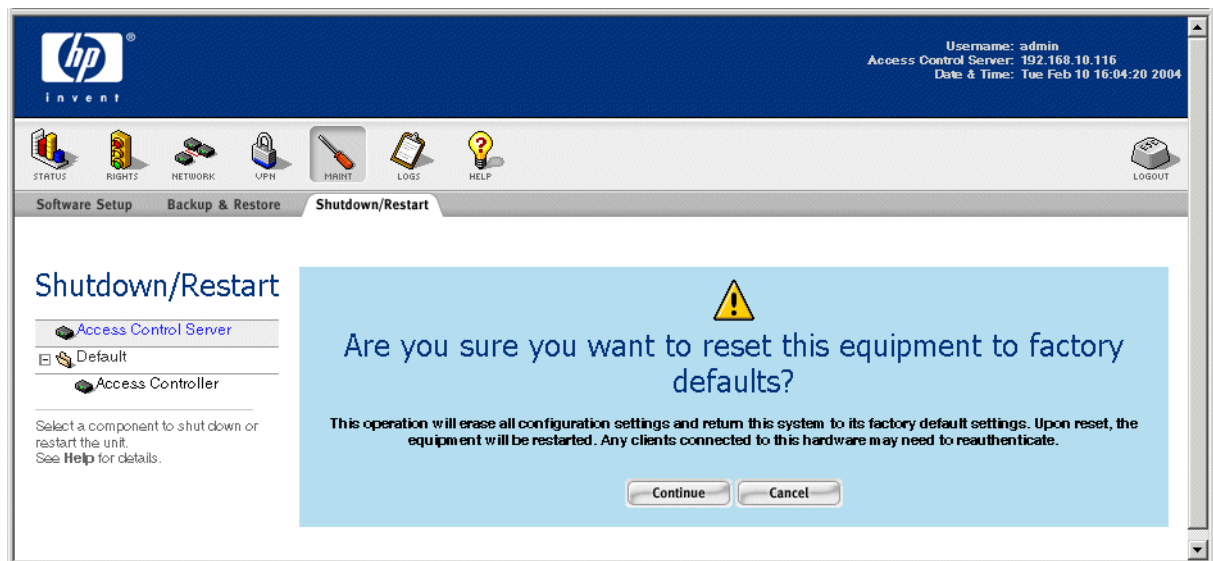
To reset a selected system component to use the factory default configuration settings:

Step 1. Select the unit you want to reset from the System Components List

Step 2. Click **Reset Now**.

A confirmation page appears, as shown in Figure 8-15.

Figure 8-15. Reset to Factory Defaults Confirmation



Step 3. To proceed with the reset, click **Continue**.

To cancel the reset, click **Cancel**.

Caution: *When 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*

System Maintenance

*restore your configuration, you must restore from a backup image that was created **and saved to an external file** before the reset. A reset erases the backup image stored on the unit.*

On an Access Controller, however, if you have not deleted the Access Controller from the Access Control Server's System Components list, as soon as the Access Controller reconnects to the Access Control Server, the Access Control Server will push the most recent Access Controller configuration information to the Access Controller. This effectively returns the Access Controller configuration to its state prior to the Reset to Factory Defaults action. If you want the Access Controller to retain the factory default settings after reconnecting to the Access Control Server, you must delete the Access Controller from the Access Control Server's System Components list before you set the Access Control Server IP address and shared secret on the Access Controller. Then when the Access Controller reconnects the Access Control Server will treat it like a new (previously unknown) Access Controller.

LOGS

This chapter presents tasks you can perform with these types of logging.

Viewing 700wl Series System Logs	9-1
Configuring Session Logging	9-4
Viewing the Session Logs	9-6
The Session Log Entry Format	9-6

Logging in the 700wl Series system can be used for accounting and troubleshooting. There are two types of logging that can take place in the 700wl Series system:

- 700wl Series system logging
- Session logging

The 700wl Series system automatically keeps log entries for a number of events from all components in the system: client logons and logoffs, errors, reboots, software upgrades, and so on. You can view all entries in the log, or tailor your view to see entries for individual units, time frames, message categories and severities, and so on (see “Viewing 700wl Series System Logs”).

Note: *Accurate time and date reporting is necessary for logs. To set the time and date, use the Date & Time tab under the **Network** pages.*

Viewing 700wl Series System Logs

Log entries from all components connected to the Access Control Server are logged into a central log database. The **LOGS** function will show you the system log file warnings and messages.

The Access Control Server or Integrated Access Manager and each Access Controller logs events to the central log file. Viewing these logs provides important information on the activity of the 700wl Series system.

- » To view the 700wl Series system log file, click **LOGS** in the Navigation bar.

The Log Files tab appears with a default view of the log file, as shown in Figure 9-1.

Logs

Figure 9-1. Log file display

The screenshot shows the HP ProCurve Secure Access 700wl Series Management and Configuration Guide interface. At the top, the HP logo and 'invent' tagline are visible. The user is logged in as 'admin' with access control server '192.168.10.116' on 'Tue Feb 10 17:31:04 2004'. The navigation bar includes icons for STATUS, RIGHTS, NETWORK, VPN, MAINT, LOGS, and HELP. The main content area is titled 'Log Files' and shows a table of log entries. The table has three columns: Time, Severity, and Message. The left-hand sidebar contains filtering options: Search (text input), Show (dropdown menu with 'All Severities' selected), Within 24 hours (dropdown menu), All Systems (dropdown menu), 25 rows per page (dropdown menu), and Auto Refresh Off (checkbox). The 'Apply Filters' button is at the bottom of the sidebar. The table displays the following log entries:

Time	Severity	Message
System	Category	
2004-02-10 16:57:55 192.168.10.68	Minor Info	NTP daemon: the system clock has been adjusted by -0.486734 seconds
2004-02-10 16:48:59 localhost	Minor Info	CS DBCACHE: xml updated 6 entries
2004-02-10 16:48:47 localhost	Major Info	CLOGSRV: central log server service started
2004-02-10 16:48:46 localhost	Minor Info	CLOGSRV: log database contains 4115 log events (at startup)
2004-02-10 13:16:34 localhost	Major Info	process 199 shutting down for backup operation, version 4.0.3.9
2004-02-10 13:16:34 localhost	Major Info	RPC initiated reboot: create backup
2004-02-10 13:06:34 localhost	Minor Info	CS DBCACHE: xml updated 6 entries
2004-02-10 12:47:12 192.168.10.68	Major Info	NTP daemon: the system clock has been adjusted by 2.391090 seconds
2004-02-10 12:30:30 192.168.10.68	Minor Info	DHCP client: lease for 192.168.10.68 to be renewed in 10944 seconds
2004-02-10 12:30:29 192.168.10.68	Minor Info	DHCP client: received DHCPACK from 192.168.2.248
2004-02-10 12:30:29 192.168.10.68	Minor Info	DHCP client: sending DHCPREQUEST to 192.168.2.248
2004-02-10 12:04:02 localhost	Minor Info	DHCP client: lease for 192.168.10.116 to be renewed in 12211 seconds
2004-02-10 12:04:01 localhost	Minor Info	DHCP client: received DHCPACK from 192.168.2.248
2004-02-10 12:04:01 localhost	Minor Info	DHCP client: sending DHCPREQUEST to 192.168.2.248
2004-02-10 11:56:36 192.168.10.68	Minor Info	NTP daemon: the system clock has been adjusted by -1.119264 seconds
2004-02-10 09:20:03 192.168.10.68	Minor Info	DHCP client: lease for 192.168.10.68 to be renewed in 11426 seconds

The Log File display table shows the log entries that exist at the moment you request the display. By default, the list is not refreshed unless you request a new display by clicking the **Apply Filters** button. You can set an automatic refresh interval using the filter settings described below.

Clicking the **LOGS** icon or the **Log Files** tab again also refreshes the page, but you lose any filter settings you may have selected previously.



The left hand column of the interface provides a number of filtering options, and also provides the following summary statistics:

Table 9-1. Log file display

Summary	Description
Messages in filter	The number of messages in the log file display based on the current filter settings.
Messages in log	The total number of messages in the log file

The log file display itself shows the following information:

Table 9-2. Log file display

Column	Description
(empty)	This column is used to call attention to log entries with severity levels or Critical or Major. Entries at lower severity levels are not flagged.
 	<ul style="list-style-type: none"> • The red octagon indicates an entry with severity level Critical • The yellow triangle indicates an entry with severity level Major
Time/Access Controller	The date and time the message was entered into the log, and below it the Access Controller from which the entry was received. You can sort by either time or Access Controller by clicking the appropriate part of the column heading.
Severity/Category	<p>The top entry is the severity level of the entry.</p> <p>The second entry is the category of the entry.</p> <p>Severity levels are:</p> <ul style="list-style-type: none"> •Critical •Major •Minor •Trivial •Never <p>Categories are:</p> <ul style="list-style-type: none"> •Error •Info •Debug •Function Trace •Object Trace •Session Log
Message	A text message that describes the reason for the log entry. This field can be searched for a word or phrase using the Search field described below.

- » To sort entries in the list, click the name of a list column— **Time**, **Access Controller**, **Severity**, **Category**, or **Message**—to sort it by that attribute. Click a second time to reverse the sort order (descending rather than ascending).

Initially the entries are sorted by time, showing the most recent entries first. The sorting functions sort the displayed entries as filtered.

- » To search for a word or phrase that you’re looking for in a message, type the word or phrase in the box under **Search**, then click **Apply Filters**.
- » To filter and display a subset of the log file entries, use the drop-down lists of filtering settings under the **Show** heading, then **Apply Filters**.

You can filter using the following attributes:

- **Severity**: All Severities (initial default), Critical, Major, Minor, Trivial, Never. Messages are caught in the filter that have a severity at or above the chosen severity—for example, the tab displays Critical and Major severity messages after you choose Major and click **Apply Filters**.

Logs

- **Categories:** All Categories (default), Error, Info, Debug, Function Trace, Object Trace, Session Log. This is a multiple selection box—by using CTRL-click or Shift-click you can select multiple categories to include in a single filter.
- **Access Controllers:** All Systems (default), localhost (the Access Control Server whose Administrative Console you are using) or the name of an individual Access Controller as shown in the System Components List

Note: *This list includes all systems for which entries exist in the logs. Therefore, an Access Manager may appear in this list even after it has been removed from the 700wl Series system and deleted from the System Components List.*

- **Time span:** Within 24 hours (default), Within 48 hours, Within 1 week, Within 2 weeks, Within 1 month
- » To change the number of log entries displayed per page, select a page height in rows per page: 25 (the default), 50, 75, 100 or 1000.
If there are more entries than can be displayed on a single page, a set of page navigation controls are displayed at below the bottom right corner of the list.
- » To refresh the list of log entries at a regular interval, select a refresh interval from the drop-down list and click **Apply Filters**. The default is no refresh (**Auto Refresh Off**) and you can select refresh intervals of 15, 30, 45, or 60 seconds.
- » Click **Clear Log** to empty the log file of older information.
- » To export a log page to file, use **Export Page as Text**. The page is displayed in a new browser window. Select **File->Save As** from the browser menu. The Save As dialog box appears. Select the file location and file type; type the file name and click **Save**.
- » To export all log pages to file, use **Export Log as Text**. The log is displayed in a new browser window. Select **File->Save As** from the browser menu. The Save As dialog box appears. Select the file location and file type, type the file name and click **Save**.

Configuring Session Logging

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

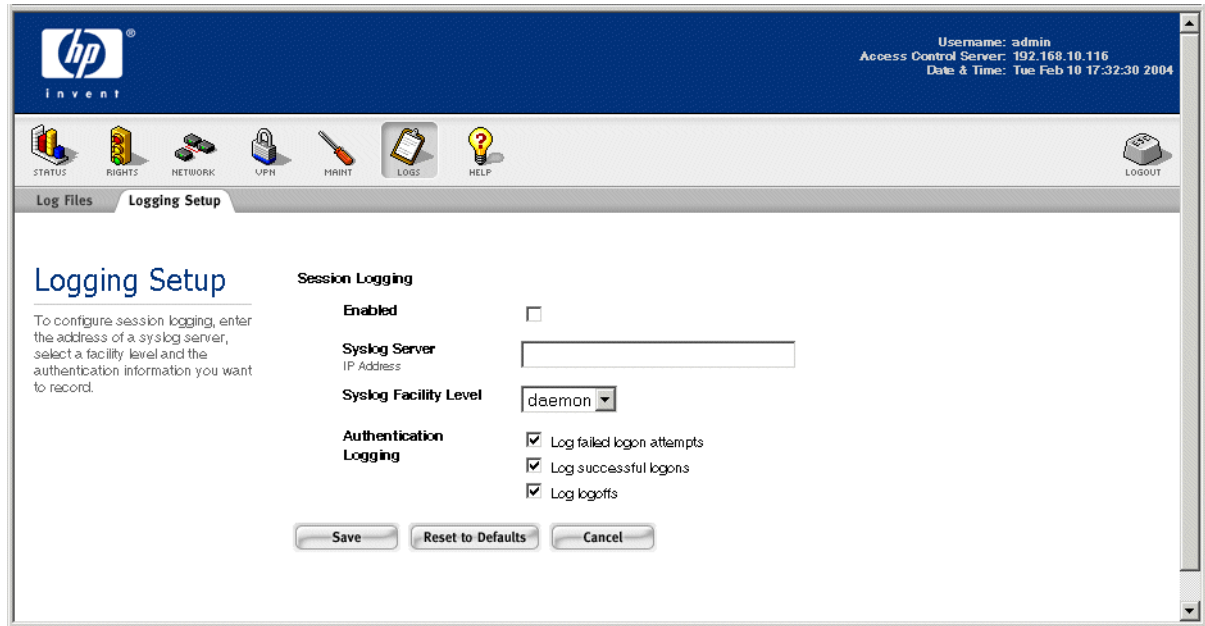
Session logging is separate from the system Log File and the status information that you can see through the Status module. The system log file keeps log entries for events, such as errors, reboots, software upgrades, and so on. Session logging keeps information about client sessions such as the date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

To specify session logging:

Step 1. Click **Logs** in the Navigation bar, then select the **Logging Setup** tab.

The Logging Setup page appears, as shown in Figure 9-2.

Figure 9-2. Setting Up Session Logging



Step 2. Type the information and select options as defined in Table 9-3.

Table 9-3. Logging Setup Fields

Field/Option	Description
Session Logging: Enabled	Settings for session logging to a remote syslog server. Check Enabled to enable session logging. Unchecking this option disables session logging without unconfiguring the syslog settings.
Syslog Server	The IP Address of the remote Syslog Server.
Syslog Facility Level	The Syslog facility appropriate for your Syslog server. You can choose Daemon, User, or Local 0 through 7.
Authentication Logging	These setting determine what authentication events are logged. Select the events that you want to include in the log file. These may include some or all of the following: <ul style="list-style-type: none"> • Log failed logon attempts • Log successful logons • Log logoffs The default is to include all events.

Step 3. When finished, click **Save**.

To restore the syslog fields to the original default settings, click **Reset to Defaults**.

To abandon your changes click **Cancel**.

The information logged to the Syslog file is described in “The Session Log Entry Format” on page 9-6.

Note: Accurate time and date reporting is necessary for accurate and useful logs. To set the time and date, use the **Date & Time** tab in the **Network** area.

Viewing the Session Logs

The 700wl Series system log files provide informational messages, warnings and so on about the operation of the 700wl Series system. Session logging goes further to provide information about every completed session. These logs are optional. If enabled, log entries are sent to an remote Syslog server that you specify when you enable session logging. For information on enabling session logging, see “Configuring Session Logging” on page 9-4.

You cannot view the session log files from the Administrative Console. You must view them on your Syslog server, or through the optional Log Analysis System, a separate application that provides powerful data analysis tools for viewing and analyzing session log data.

You can view session status for an individual client under the Session Status tab in the Status module of the Administrative Console. See “Viewing Session Status” on page 3-12 for more information.

The Session Log Entry Format

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

```
logmsg: pri 36, flags 0, from vm18.testbed.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 (the underlined fields 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 data 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 9-4 defines the items in the session log entry. The items are delimited by spaces.

Table 9-4. 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

Table 9-4. Session Log information

Data Item	Definition
Actual Destination	The actual destination IP address and port, if redirected or tunneled 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> <Access Controller IP> <slot>/<port>
and
disassoc <client MAC> <Access Controller IP>
```

Associate messages are sent to the Access Control Server 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 "Client Polling" on page 6-25" for a more detailed discussion of client disassociation.)

You cannot view the session log from the 700w1 Series system Administrative Console. 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 Session Status" on page 3-12.

Logs

A

COMMAND LINE INTERFACE

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 700wl Series system.

The Command Line Interface commands are listed in the following categories:

Accessing the Command Line Interface	A-2
Getting CLI Command Help	A-3
Administrator Access Control Commands	A-4
System Status and Information Commands	A-6
Network Configuration Commands	A-9
Port Configuration Commands	A-12
Access Controller Configuration	A-14
Access Control Server Configuration	A-15
Remote Commands	A-18
Wireless Data Privacy Configuration	A-21
Active Client Management Commands	A-23
System Backup, Upgrade and Shutdown Commands	A-25
Diagnostic and Log Commands	A-30
Time Configuration	A-33
SNMP Configuration and Reporting Commands	A-34

Note: You can also perform these functions through the Administrative Console on the Access Control Server.

For an alphabetical listing of commands see the “Index of Commands” at the back of this manual.

Note: Only a subset of these commands are supported on an Access Controller. Access Controller configuration changes should be performed through the Administrative Console from the managing Access Control Server.

Accessing the Command Line Interface

There are two ways to access the Command Line Interface—either by directly connecting a serial console to the serial port on an Access Controller, Access Control Server, or Integrated Access Manager, or by connecting to the system remotely using SSH.

Connecting with a Serial Console

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 700w1 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
```

Connecting Using SSH

You can access the Command Line Interface on a 700w1 Series system unit over the network, rather than by connecting to the serial port, by connecting via SSH to the IP address of the unit at port 22. You log in using the built-in administrator username and password for the unit (by default this is username *admin*, password *admin*).

Note: *There are a number of commands, executed either from the CLI or from the Administrative Console, that cause a global restart and will terminate a running SSH session. These include commands such as changing the NAT DHCP settings, enabling or disabling SSH for Wireless Data Privacy, changing the Access Control Server IP address on an Access Controller, or enabling or disabling Technical Support access. In addition, upgrading a flash-based Access Controller shuts down the SSH subsystem.*

Using the CLI on an Integrated Access Manager

Within the CLI, some commands are supported only on an Access Control Server, others only on an Access Controller. An Integrated Access Manager includes both Access Control Server and Access Controller functionality, but each portion functions independently. In order to execute Access Control Server-only commands on an Integrated Access Manager, you must be connected to the Access Control Server portion. Likewise, you must connect to the Access Controller portion to execute Access Controller-only commands.

The CLI provides two commands, **cli ACS** and **cli AC**, to connect you to the Access Control Server or Access Controller portions of an Integrated Access Manager. To execute Access Controller-only commands, you must first connect to the Access Controller portion with the **cli AC** command. To subsequently execute Access Control Server-only commands, you must reconnect to the Access Control Server portion with the **cli ACS** command.

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 A-1 summarizes command syntax symbols.

Table A-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 <code>set datetime <date> <time></code> 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 <code>logoff client {all mac <mac-address>}</code> 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 <code>set dhcp on off</code> you can enter <code>set dhcp on</code> or <code>set dhcp off</code> . 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 <code>set dns <ip-address> [<ip-address>]</code> 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 press 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 ?
```

Command Line Interface

This produces the following output:

```
"add" commands:
  add bridging ...           Add bridging options
  add snmpmanager ...       Add an SNMP authorized manager
  add snmptrapreceiver ...   Add 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. These commands are supported on Access Controllers as well as on the Access Control Server or Integrated Access Manager.

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

Resets the console and web administrator login and password to the factory default ("admin" and "admin"). You are prompted to confirm before this action is taken.

cli AC | ACS

Connects the CLI to either the Access Controller or Access Control Server command environment of an Integrated Access Manager.

On an Integrated Access Manager, the Command Line Interface can communicate with both the Access Control Server and the Access Controller portions of the system, but cannot do so concurrently. When you first log onto an Integrated Access Manager, the CLI connects to the Access Control Server portion of the system.

cli AC sets the CLI to connect to the Access Controller portion of the Integrated Access Manager.

cli ACS sets the CLI to connect to the Access Control Server portion of the Integrated Access Manager.

exit

Logs you off of the system, whether an Access Control Server, an Access Controller, or an Integrated Access Manager.

show admin

Shows the current administrator login. The password is not displayed.

set superadmin pass | enable | disable <login>

Set the password for a superadmin. Enable or disable a superadmin login.

pass	Change the password for the specified login name. The superadmin can change any password.
enable	Enable the specified login name. Only superadmins can enable admins.
disable	Disable the specified login name. Only superadmins can disable admins.
<login>	Login name of a superadmin.

delete superadmin <login>

Delete a superadmin with the specified login. This command is only available to superadmins.

show superadmin [<login>]

Show a specific superadmin by specifying a login, or list all superadmins by not specifying a login.

set networkadmin pass | enable | disable <login>

Set the password for a networkadmin. Enable or disable a networkadmin login.

pass	Change the password for the specified login name. The superadmin can change any password. A networkadmin may only change their own password.
enable	Enable the specified login name. Only superadmins can enable admins.
disable	Disable the specified login name. Only superadmins can disable admins.
<login>	Login name of a networkadmin.

delete networkadmin <login>

Delete a networkadmin with the specified login. This command is only available to superadmins.

show networkadmin [<login>]

Show a specific networkadmin by specifying a login, or list all networkadmins by not specifying a login.

set policyadmin pass | enable | disable <login>

Set the password for a policyadmin. Enable or disable a policyadmin login.

pass	Change the password for the specified login name. The superadmin can change any password. A policyadmin may only change their own password.
enable	Enable the specified login name. Only superadmins can enable admins.
disable	Disable the specified login name. Only superadmins can disable admins.
<login>	Login name of a policyadmin.

delete policyadmin <login>

Delete a policyadmin with the specified login. This command is only available to superadmins.

Command Line Interface

show policyadmin [<login>]

Show a specific policyadmin by specifying a login, or list all policy admins by not specifying a login.

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.

set sshcli on | off

Enables or disables the Access Control Server or Access Controller to act as an SSH server, allowing users to connect the command line interface using an SSH client. If you are using the CLI in via an SSH client and issue the command **set sshcli off**, your SSH session will be terminated and you will be logged off of the system.

show sshcli

Shows the current SSH settings for the command line interface. For example:

```
show sshcli
```

```
SSH CLI remote access is enabled.
```

or

```
SSH CLI remote access is disabled.
```

System Status and Information Commands

show status

Displays an overview of the system status.

- For an 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 its Access 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
  Access Control Server:  Use Integrated Server
  Active Clients:  None
Access Control Server Function
  Enabled:          Yes
  Access Controllers:  1 connected
  MAC Address      IP Address      Connected
```

```
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 Slot 0 port 1.

On a 700wl Series unit, the default uplink port is slot 0 port 2. (Slot 0 port 1 is the Reserved port.) Therefore, the MAC address of the uplink port, shown on the label on the back of the unit, will be one higher than the MAC address used as the system ID.

For example, if the label on the back of your 700wl Series unit showed 00:E0:18:50:1D:AC as the MAC address (for the uplink, slot 0 port 2) then the **show id** command would display 00:E0:18:50:1D:AB as the system ID. This ID is also displayed when you first logon through the serial console.

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

Slot 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:

```
System Board: 1 Ethernet port
  0/1: 00:e0:18:7d:b5:3d, autoselect (100baseTX <full-duplex>), active

Slot 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
System Board: 2 Ethernet ports
Slot 1: Empty
Slot 2: 4 Ethernet ports
Slot 3: 4 Ethernet ports
```

Command Line Interface

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 760w1 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 760w1, 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:

Version	Build Date	Install Date	
-----	-----	-----	
Active: 3.1.43	Feb 24 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

refresh client all | [mac <mac-address>]

Note: This command is supported on the Access Control Server or Integrated Access Manager only.

Refreshes the rights for a specific client, identified by MAC address, or for all clients. The command **refresh client all** refreshes the rights of all the clients on the 700w1 Series system.

Network Configuration Commands

set hostname <hostname>

Note: This command is supported on the Access Control Server or Integrated Access Manager only.

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

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

Clears the system's hostname.

set domainname <domainname>

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

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

Note: This command is supported on the Access Control Server or Integrated Access Manager only.

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.

Command Line Interface

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>

Note: This command is supported on the Access Control Server or Integrated Access Manager only.

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

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

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>]

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

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

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

Clears the IP addresses of the DNS servers.

set sharedsecret [<secret> <secret>]

Sets the shared secret used to validate a connection between an Access Controller and Access Control Server. Prompts for the secret if not entered on the command line.

Note: Once a connection has been established between an Access Controller and its Access Control Server (or Integrated Access Manager), changing the shared secret on either unit does not disrupt this communication. To disconnect an Access Controller from an Access Control Server, you must both change the shared secret and change the Access Control Server IP address configured in the Access Controller.

clear sharedsecret

Clears the shared secret.

show sharedsecret

Shows whether the 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
```

set wins <primary-ip-address> [<secondary-ip-address>]

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

Command Line Interface

Sets the IP addresses of the WINS servers.

<primary-ip-address> The IP address of the primary WINS server for the system.

<secondary-ip-address> The IP address of the secondary WINS server for the system (optional).

clear wins

Note: This command is supported on the Access Control Server or Integrated Access Manager only. For an Access Controller, this function must be performed through the Administrative Console on the managing Access Control Server.

Clears the IP addresses of the WINS servers.

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 network uplink port to the specified port or slot and port. <slot>/<port> specifies the port on a Gigabit Ethernet option card. For a single-port card, the port number is 1.

There is a delay of several seconds 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:

- 0/2 (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.

Note: You will need to reboot your system for uplink changes to take effect.

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
```


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 <code>100baseTX</code> or <code>10baseT/UTP</code> . Must match one of the valid media types for the port, as displayed in the <code>show portmedia</code> command for the port.
<media-option>	A media option, for example <code>full-duplex</code> . 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 <code>show portmedia</code> command for the port.

You can use the **show portmedia** command to get a list of supported media and media option settings.

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
    Port status: active
    Configured setting: autoselect
    Active port setting: 100baseTX full-duplex
    Supported settings: autoselect
                        100baseTX full-duplex
                        100baseTX
                        10baseT/UTP full-duplex
                        10baseT/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 Notices).

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.

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 Status Commands

The following commands are available only from an Access Controller or Integrated Access Manager.

Command Line Interface

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
Slot 1 Port 1  IP: Not set
Slot 1 Port 2  IP: 192.168.5.1      Netmask: 255.255.255.0
Slot 1 Port 3  IP: 192.168.6.1      Netmask: 255.255.255.0
Slot 1 Port 4  IP: Not set
Slot 2 Port 1  IP: Not set
Slot 2 Port 2  IP: Not set
Slot 2 Port 3  IP: Not set
Slot 2 Port 4  IP: Not set
Slot 3 Port 1  IP: Not set
Slot 3 Port 2  IP: Not set
Slot 3 Port 3  IP: Not set
Slot 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 accesscontrolserver**, **clear accesscontrolserver**, and **show accesscontrolserver** commands, which are not available on an Integrated Access Manager. None of these commands are available on an Access Control Server.

Note: To disconnect an Access Controller from an Access Control Server, you must first change the shared secret then the Access Control Server IP address. If you change the Access Control Server IP address without changing the shared secret, the synchronization function between the Access Control Server and the Access Controller will reset the Access Control Server IP address back to the original Access Control Server IP address.

set accesscontrolserver <ip-address>

On an Access Controller, sets the IP address of its Access Control Server or Integrated Access Manager.

Note: This command is not available on an Integrated Access Manager.

clear accesscontrolserver

On an Access Controller, clears the Access Control Server or Integrated Access Manager IP address.

Note: This command is not available on an Integrated Access Manager.

show accesscontrolserver

On 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 Status

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 "Bridging" on page 6-24 in Chapter 6, and Appendix B, "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:
  cdp: ether [12:2] <= 1514 and ether dst 01:00:0c:cc:cc:cc
  wnmp: ether [12:2] = 0x8781 and ether[0:4] = 0x01a0f8f0
  custom: ether[12:2] = 0x8037 or ether[12:2] = 0x8137
```

show clientprobes

Displays the current configuration of the client probe timers. Output from this command is similar to the following:

```
Client probes
  Interval: 30 seconds of idle time
  Timeout: 300 seconds of idle time
```

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 an Access Control Server or an Integrated Access Manager in **cli ACS** mode, except for the **show syslogserver** and **show natdhcp** commands, which are also available on an Access Controller.

Command Line Interface

show ac [mac <mac-address>]

Shows Access Controller settings for one or all Access Controllers connected to the Access Control Server or Integrated Access Manager. The default is to show all settings for all Access Controllers.

mac <mac-address> Specifies the MAC address of an Access Controller

The **show ac** 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.

enable redundancy

Enables Access Control Server failover in the 700w1 Series system. Redundancy (failover) will be enabled with the current parameters. These can be displayed by using the command **show redundancy**. The parameters can be set using **set redundancy**.

Note: If you set a redundant peer IP address, there is a seven second configuration change delay before the change takes effect. If you try to enable redundancy before seven seconds have elapsed, the enable command will fail with a message that no peer is specified.

disable redundancy

Disables the redundancy system.

set redundancy [peer <peer ip-address>] | [priority <priority value>] | [retry <retry time>] | [failover <failover time>]

Sets the parameters for redundancy (failover). You set one parameter at a time. The possible settings are:

- peer <peer ip-address> Sets the IP address for a redundant peer.
After a seven second configuration change delay, this Access Control Server will attempt to contact the specified peer.
- priority <priority value> Sets the 16 bit signed peer priority value for this Access Control Server.
- Range is -32768 - +32767. The Access Control Server with the lowest value is taken as the preferred primary Access Control Server in case of failover.
 - If the priority is set through the Administrative Console, a value of -10 (negative ten) indicates the Access Control Server has been designated as the preferred primary. A peer that is not designated the preferred primary has a priority of zero (0).
- retry <retry time> Sets the retry time, in seconds. The retry time specifies the time interval between attempts to reconnect to a disabled peer.
- failover <failover time> Sets the failover time, in seconds. This time interval determines how long an Access Control Server waits for a response from its peer before determining that the peer has failed and initiating failover.
- Note:** If redundancy is currently enabled, you cannot change the failover time.

show redundancy

Shows the current redundancy (failover) settings. For example:

```
show redundancy

---- Redundancy configured state ----
Redundancy is disabled.
No peer is specified.
Peering priority is 0.
Retry timeout to disabled peers is 60 seconds.
Failover timeout is 30 seconds.
```

On an Access Control Server acting as the secondary Access Control Server, the show redundancy command produces output similar to:

```
---- Redundancy configured state ----
Redundancy is enabled.
Redundant peer is 192.168.10.82.
Peering priority is 0.
Retry timeout to disabled peers is 60 seconds.
Failover timeout is 30 seconds.
---- Redundancy running state ----
We are secondary to peer 192.168.10.82
Peer is responding
```

The redundancy settings can be changed using the command **set redundancy**. To enable redundancy, use the **enable redundancy** command.

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 an 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 <code>seconds</code> , <code>minutes</code> , <code>hours</code> , <code>days</code> , <code>weeks</code> , or <code>months</code> . Default is <code>seconds</code> .

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
```

Remote Commands

The following commands are available only on an Access Control Server or Integrated Access Manager in **cli ACS** mode. These commands allow the administrator to perform functions on a remote Access Controller or peer Access Control Server through the CLI. The system at the specified IP address must be one that the Access Control Server can manage—i.e. the remote system must be configured with this Access Control Server's IP address and shared secret.

remote ping <ip-address>

Pings the Access Controller at <ip-address> via the control channel.

remote cancel <ip-address>

Cancels the upgrade occurring on the Access Controller or secondary Access Control Server at <ip-address>.

remote datetime <ip-address> <date> <time>

Sets the date and time on the system at <ip-address>.

<date> The current date in yyyy/mm/dd format

<time> The current time in h24:mm format.

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 potential disruptions.*

remote sysinfo <ip-address> [<item>]

Shows status information about the system at the specified IP address. If no <item> is included, all system info is presented.

<item> Specifies a specific item to be reported. May be one of the following:

- cur_version: the current (running) software version
- alt_version: the alternate software version
- cur_install: the date and time the current version was installed
- alt_install: the date and time the alternate version was installed
- cur_time: the system date and time
- start_time: the date and time the system was last booted
- backup_time: the date and time the last backup was created
- min_downgrade: the oldest version to which the remote system may be downgraded without requiring a factory reset.

If no parameter is included, output is as follows:

```
remote sysinfo 192.168.10.68

Remote Info for 192.168.10.68:
  System Boot Time:      Oct 13 15:38:09 2003
  System Current Time:   Oct 13 18:10:26 2003
  System Backup Time:    Dec 31 16:00:00 1969
  Current Version:       3.5.238
  Current Install Time:  Oct 13 15:36:17 2003
  Alternate Version:     3.5.234
  Alternate Install Time: Oct 10 10:47:02 2003
  Min Downgrade Ver:    3.5.141
```

The following is an example of a specific item request:

```
remote sysinfo 192.168.10.68 cur_install

Remote Info for 192.168.10.68:
  Current Install Time:  Oct 13 15:36:17 2003
```

Command Line Interface

remote reboot <ip-address>

Reboot the system at <ip-address>

remote rebootalt <ip>

Reboot the system at <ip-address> to alternate software version.

remote shutdown <ip-address>

Shutdown the system at <ip-address>

remote factoryreset <ip-address>

Factory reset the system at <ip-address>

remote upgrade <ip-address> <url> <key>

Upgrade the system at the specified IP address.

<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.

remote upgradereboot <ip-address> <url> <key>

Upgrades the system at the specified IP address and reboots the system.

<url>	<p>The URL encoded location of the software release to install. The format of the URL is <code><protocol>://<host>/<update file></code> or <code><protocol>://<username>[:<password>]@<host>/<update file></code></p> <p><code><protocol></code> can be <code>ftp</code>, <code>http</code>, or <code>tftp</code>.</p> <p><code><username>[:<password>]</code> specifies a username and optional password with access to the remote site, if required.</p> <p><code><update file></code> 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.</p> <p>The host must be an FTP, HTTP or TFTP server.</p>
<key>	<p>The software release install key obtained from HP ProCurve.</p>

remote upgradecheck <ip-address> <url>

Checks whether an upgrade is available for the system at the specified IP address. No key is required for this operation.

<url>	<p>The URL encoded location of the software release to install. The format of the URL is <code><protocol>://<host>/<update file></code> or <code><protocol>://<username>[:<password>]@<host>/<update file></code></p> <p><code><protocol></code> can be <code>ftp</code>, <code>http</code>, or <code>tftp</code>.</p> <p><code><username>[:<password>]</code> specifies a username and optional password with access to the remote site, if required.</p> <p><code><update file></code> 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.</p> <p>The host must be an FTP, HTTP or TFTP server.</p>
--------------------	--

remote upgradestatus <ip-address>

Get the upgrade status of the system at `<ip-address>`

Wireless Data Privacy Configuration

Wireless Data Privacy is configured and maintained centrally on an 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 vpn** command, are not available on an Access Controller.

Command Line Interface

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 | off

Enables or disables IPsec.

set initialcontact on | off

Enables or disables IPsec initial contact messages to clients. Enabled by default.

set ssh on | off

Enables or disables ssh for Wireless Data Privacy.

show vpn

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 vpn` 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
```

Active Client Management Commands

Use the **show clients** command to manage Active Clients from an Access Control Server or an Integrated Access Manager (in **cli cs** mode).

show clients [**<filter>**] [**sort <sort>**] [**reverse**]

Lists all active clients. You can optionally filter by mac address, sort the list by a number of criteria, and display the list in reverse order.

filter	mac <mac>, where mac is the (Ethernet) address to display. Specified in the format: <code>xx:xx:xx:xx:xx:xx</code> or <code>xxxxxxxxxxxx</code> (colons are optional).
sort	Sort the clients according to one of the following criteria: <ul style="list-style-type: none"> • <code>am_ip</code>: by IP address of the Access Controllers • <code>am_mac</code>: by the mac address of the Access Controllers • <code>mac</code>: by MAC address (This is the default sort value if none is specified and the sort keyword is used.) • <code>nat_ip</code>: by NAT'ed IP addresses • <code>port</code>: by Access Controller port • <code>real_ip</code>: by IP address given to client by DHCP (as opposed to NAT'ed) • <code>ip</code>: by IP address • <code>state</code>: by logged on state • <code>user</code>: by user name
reverse	Keyword that reverses the order of the display, which normally displays the most recent events first (in ascending order).

Use the commands listed below to manage Active Clients from an Access Controller or Integrated Access Manager (in **cli am** mode). These commands cannot be used from an Access Control Server.

Command Line Interface

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 xxxxxxxxxxxxxx (colons are optional).
sort	Sort the clients according to one of the following criteria (one must be specified): <ul style="list-style-type: none">• 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> [rights]

Lists active sessions for a client. Shows client rights if requested.

mac	<mac>, where mac is the (Ethernet) address to display. Specified in the format: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxxxx (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 xxxxxxxxxxxxxx (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]?

```

Command Line Interface

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.

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.

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/software/700software/ambit4-hp
```

For a flash-based Access Controller, the default URL is:

```
ftp://ftp.hp.com/pub/networking/software/700software/ambit4-ac-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).

Note: *The mindowngrade version applies to this unit only and does not check for compatibility against all other units in your system.*

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.

Command Line Interface

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 <i>without</i> 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 warning message appears. For example, suppose you want to upgrade a system that is currently running version 3.1.122, and the upgrade available at the URL you provide is 4.0.12. The get upgrade command will return a warning similar to the following:

```
Minimum downgrade for the version at that URL: 4.0.0  
Installed version: 3.1.122  
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: 4.0.0
```

- 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: 3.1.122)
```

Caution: *If you upgrade or downgrade a unit to a version that is substantially different from the software version running on other units in your 700wl Series system, those units may not be able to communicate. See the release notes for the affected software versions for possible information on compatibility across the 700wl Series system between software versions. In particular, units running software version 4.0 cannot communicate with units running software version 3.1 or earlier.*

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.

Command Line Interface

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 DHCP OFFER 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 2.1.534
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.

Command Line Interface

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

The following commands are available only on an Access Control Server or an Integrated Access Manager in **cli ACS** mode, except for the **show time** command, which is also available on an Access Controller. To modify these settings on an Access Controller, you must use the Administrative Console on the managing Access Control Server.

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.

Command Line Interface

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.

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 potential disruptions.*

show time

Note: *Even though you can only configure the time and timezone of an Access Controller from an Access Control Server or Integrated Access Manager, you can use the **show time** command from an Access Controller to view the time and timezone settings.*

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 Console or the CLI.*

The following commands are available only on an Access Control Server or an Integrated Access Manager in **cli ACS** mode, except for the **show snmp** command, which is also available on an Access

Controller. To modify these settings on an Access Controller, you must use the Administrative Console on the managing Access Control Server.

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> [/<mask>]

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> [/<mask>]

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.

Command Line Interface

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

Note: Even though you can only configure SNMP for an Access Controller from an Access Control Server or Integrated Access Manager, you can use the **show snmp** command from an Access Controller to view the SNMP settings.

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

FILTER EXPRESSION SYNTAX

This appendix describes the syntax used to define user access rights (allowed traffic filters and redirected traffic filters), bridged traffic, and HTTP Proxy filters.

It includes the following sections:

Introduction	B-1
Filter Specification Syntax	B-1
Tcpdump Primitives	B-2

Introduction

The 700w1 Series system uses filters defined in `tcpdump` syntax to specify user access rights (Allowed Traffic filters and Redirected Traffic filters), 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 700w1 Series system for defining Allowed and Redirected Traffic filters, 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 the type of object to which the ID name refers. Possible types are **host**, **net** and **port**. If there is no type qualifier, **host** is assumed.

Examples are: “host myHost”, “net 122.43”, or “port 44”.

- *Direction* qualifiers specify a particular transfer direction— from the ID (**src**), to the ID (**dst**), either to or from (**src or dst**) or both to and from (**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 myHost”, “dst net 122.43”, or “src or dst port ftp-data”.

- *Protocol* qualifiers restrict the match to a particular protocol. Possible protocols are: **ether**, **fddi**, **tr**, **ip**, **ip6**, **arp**, **rarp**, **decnet**, **tcp** and **udp**. If there is no protocol qualifier, all protocols consistent with the ID type are assumed.

Examples are: "fddi src myHost", "ip net 122.43", and "udp port 44".

fddi is an alias for **ether**; they are treated identically as meaning "the data link level used on the specified network interface." FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just as with the analogous Ethernet fields. (FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression.)

Similarly, **tr** is also an alias for **ether**; the previous paragraph's statements about FDDI headers also apply to Token Ring headers.

- In addition to the above, there are some special primitives: **gateway**, **broadcast**, **multicast**, **vlan**, **less**, **greater** and arithmetic expressions. All of these are described in Table B-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").
- Intersection or logical AND ("&&" or "and").
- Union or logical OR ("||" or "or").

Negation has highest precedence. Intersection and union have equal precedence and associate left to right. There is no implicit logical AND'ing by concatenation; you must explicitly use **and** operators.

Examples are: "not host foo", or "not port ftp or not port ftp-data", or "!(port ftp || 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 bar" is the same as "not host foo and host bar". Both are true if the packet includes host bar 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 either host foo or host ace are the source or destination of the packet.

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 B-1. For more details refer to the UNIX man page tcpdump, and other related man pages noted in the explanation text in Table B-1.

Note: *Tcpdump syntax is case sensitive. All keywords must be in lower-case to be recognized.*

Table B-1. Allowable Primitives

Primitive	Explanation
dst host <i>host</i>	True if the destination field of the packet is <i>host</i> , which can be either an address or a name.
src host <i>host</i>	True if the source field of the packet is <i>host</i> .

Table B-1. Allowable Primitives (Continued)

Primitive	Explanation
host <i>host</i>	True if either the source or destination of the packet is <i>host</i> .
ether dst <i>ehost</i>	True if the Ethernet destination address is <i>ehost</i> . <i>Ehost</i> can be either a name from <i>/etc/ethers</i> or a number (see <i>ethers(3N)</i> for numeric format).
ether src <i>ehost</i>	True if the Ethernet source address is <i>ehost</i> .
ether host <i>ehost</i>	True if either the ethernet source or destination address is <i>ehost</i> .
gateway <i>host</i>	True if the packet used <i>host</i> as a gateway. In other words, the ethernet source or destination address was <i>host</i> but neither the IP source nor the IP destination was <i>host</i> . <i>Host</i> must be a name and must be found both by the machine's host-name-to-IP-address resolution mechanisms (host name file, DNS, NIS, etc.) and by the machine's host-name-to-Ethernet-address resolution mechanism (<i>/etc/ethers</i> , etc.). (An equivalent expression is <i>ether host ehost</i> and not <i>host host</i> which can be used with either names or numbers for <i>host / ehost</i> .) This syntax does not work in IPv6-enabled configuration
dst net <i>net</i>	True if the destination address of the packet has a network number of <i>net</i> . <i>Net</i> can be either a name from <i>/etc/networks</i> or a network number (see <i>networks(4)</i> for details).
src net <i>net</i>	True if the source address of the packet has a network number of <i>net</i> .
net <i>net</i>	True if either the source or destination address of the packet has a network number of <i>net</i> .
net net mask <i>mask</i>	True if the IP address matches <i>net</i> with the specific netmask. Can be qualified with src or dst .
net <i>net/length</i>	True if the address matches <i>net</i> a netmask <i>length</i> bits wide. Can be qualified with src or dst .
dst port <i>port</i>	True if the packet is ip/tcp or ip/udp, and has a destination port value of <i>port</i> . The <i>port</i> can be a number or a name used in <i>/etc/services</i> (see <i>tcp(4P)</i> and <i>udp(4P)</i>). 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 <i>port</i>	True if the packet has a source port value of <i>port</i> .
port <i>port</i>	True if either the source or destination port of the packet is <i>port</i> . 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 <i>port</i> .
less <i>length</i>	True if the packet has a length less than or equal to <i>length</i> .
greater <i>length</i>	True if the packet has a length greater than or equal to <i>length</i> .
ip proto <i>protocol</i>	True if the packet is an IP packet (see <i>ip(4P)</i>) of protocol type <i>protocol</i> . <i>Protocol</i> 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 B-1. Allowable Primitives (Continued)

Primitive	Explanation
ip6 proto <i>protocol</i>	True if the packet is an IPv6 packet of protocol type <i>protocol</i> . This primitive does <u>not</u> chase the protocol header chain.
ip6 protochain <i>protocol</i>	True if the packet is IPv6 packet, and contains protocol header with type <i>protocol</i> in its protocol header chain. For example, <code>ip6 protochain 6</code> matches any IPv6 packet with TCP protocol header in the protocol header chain. The packet may contain, for example, authentication header, routing header, or hop-by-hop option header, between IPv6 header and TCP header. The BPF code emitted by this primitive is complex and cannot be optimized by BPF optimizer code in <code>tcpdump</code> , so this can be somewhat slow.
ip protochain <i>protocol</i>	True if the packet contains protocol header with type <i>protocol</i> in its protocol header chain. For example, <code>ip protochain 6</code> 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 <code>tcpdump</code> , so this can be somewhat slow.
ether broadcast	True if the packet is an Ethernet broadcast packet. The <i>ether</i> 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 <i>ether</i> keyword is optional. This is shorthand for ether[0] & 1!= 0 .
ip multicast	True if the packet is an IP multicast packet.
ip6 multicast	True if the packet is an IP6 multicast packet.

Table B-1. Allowable Primitives (Continued)

Primitive	Explanation
<p>ether proto <i>protocol</i></p>	<p>True if the packet is of ether type <i>protocol</i>. Protocol can be a number or one of the names ip, ip6, arp, rarp, atalk, aarp, decnet, sca, lat, mopdl, moprc, iso, stp, ipx, or netbeui.</p> <p>Note: Note these identifiers are also keywords and must be escaped via backslash (\).</p> <p>[In the case of FDDI (e.g., 'fddi protocol arp') and Token Ring (e.g., 'tr protocol arp'), for most of those protocols, the protocol identification comes from the 802.2 Logical Link Control (LLC) header, which is usually layered on top of the FDDI or Token Ring header.</p> <p>When filtering for most protocol identifiers on FDDI or Token Ring, tcpdump checks only the protocol ID field of an LLC header in so-called SNAP format with an Organizational Unit Identifier (OUI) of 0x000000, for encapsulated Ethernet; it doesn't check whether the packet is in SNAP format with an OUI of 0x000000. The exceptions are:</p> <ul style="list-style-type: none"> • iso, for which it checks the DSAP (Destination Service Access Point) and SSAP (Source Service Access Point) fields of the LLC header • stp and netbeui, for which it checks the DSAP of the LLC header • atalk, for which it checks for a SNAP-format packet with an OUI of 0x080007 and the Appletalk etype <p>In the case of Ethernet, tcpdump checks the Ethernet type field for most of those protocols; the exceptions are:</p> <ul style="list-style-type: none"> • iso, sap, and netbeui, for which it checks for an 802.3 frame and then checks the LLC header as it does for FDDI and Token Ring • atalk, for which it checks both for the Appletalk etype in an Ethernet frame and for a SNAP-format packet as it does for FDDI and Token Ring • aarp, for which it checks for the Appletalk ARP etype in either an Ethernet frame or an 802.2 SNAP frame with an OUI of 0x000000, • ipx, for which it checks for the IPX etype in an Ethernet frame, the IPX DSAP in the LLC header, the 802.3 with no LLC header encapsulation of IPX, and the IPX etype in a SNAP frame.]
<p>vlan [<i>vlan_id</i>]</p>	<p>True if the packet is an IEEE 802.1Q VLAN packet. If [<i>vlan_id</i>] is specified, then this is only true if the packet has the specified <i>vlan_id</i>. Note that the first vlan keyword encountered in <i>expression</i> changes the decoding offsets for the remainder of the <i>expression</i> on the assumption that the packet is a VLAN packet.</p>
<p>tcp, udp, icmp</p>	<p>Abbreviations for ip proto <i>p</i> or ip6 proto <i>p</i>, where <i>p</i> is one of the above protocols.</p>

Table B-1. Allowable Primitives (Continued)

Primitive	Explanation
<i>expr relop expr</i>	<p>True if the relation holds, where</p> <ul style="list-style-type: none">• <i>relop</i> is one of >, <, >=, <=, =, !=• <i>expr</i> 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. <p>To access data inside the packet, use the syntax <i>protocol [expr: size]</i>.</p> <p>Proto is one of ether, fddi, tr, ip, arp, rarp, tcp, udp, icmp or ip6, and indicates the protocol layer for the index operation. Note that tcp, udp and other upper-layer protocol types only apply to IPv4, not IPv6</p> <ul style="list-style-type: none">• The byte offset, relative to the indicated protocol layer, is given by <i>expr</i>.• <i>Size</i> 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. <p>The length operator, indicated by the keyword len, gives the length of the packet.</p>

CREATING CUSTOMIZED TEMPLATES

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	C-1
A Simple Logon Page Template Example	C-2
Logon Template Elements	C-3
Logon Page Template — A More Advanced Example	C-7
Changing the Logon Button Names	C-10
Using a Logoff Pop-Up with a Customized Logon Page	C-16
Customizing the Stop Page	C-19

Introduction

While the Rights Manager Logon Customization pages 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 Logon Customization feature. Custom templates allow you to create pages that meet your individual needs.

The HP ProCurve Secure Access 700wl Series system 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 under the Custom Templates tab of the New or Edit Logon Customization 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. See “Logon Page Customization” on page 5-30 for details of how to upload a custom template.

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 HP 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 C-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" on page C-3.

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=/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()

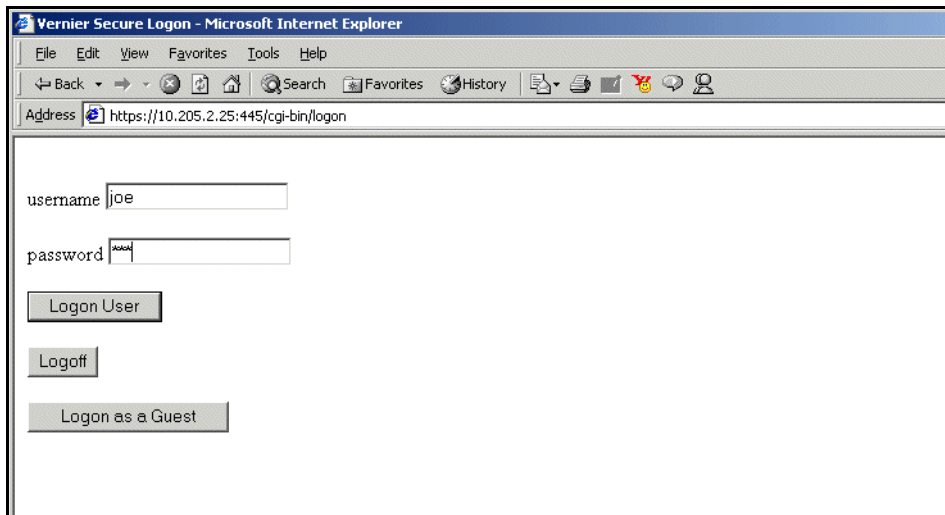
</FORM>
</body>
</html>

```

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 C-1.

Figure C-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

Form Tag

```
<FORM action=/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.

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 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.

- `@satmac()`. This function returns an INPUT element of type hidden, with a value that is the client's MAC address.
- `@interface()`. This function returns an INPUT element of type hidden.
- `@java_works()`. This function returns an INPUT element of type hidden, with a value of 0. If a Logoff popup is specified (see "Body Tag to Enable Logoff Popup" below) the value is changed by the 700wl Series system to 1.
- `@secret()`. This function returns an INPUT element of type hidden, with a value that indicates that this page has been loaded. This prevents a user from reloading this page and logging on again without the Rights Manager's knowledge.
- `@query()`. This function returns an INPUT element of type hidden, with the value passed into the HTTP request.

For example, if a user typed `www.yahoo.com` they would be redirected to `http://1.2.3.4/logon?www.yahoo.com`. In this case, the value passed into the http request is `www.yahoo.com` (in other words, everything after the question mark (?))

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

```

```

Images used by the HP 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.

Client Functions

The following functions return information from the 700wl Series system 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). <ul style="list-style-type: none">• Returns 0 if the client has expired• Returns -1 if the client never expires.

Miscellaneous 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: <code>@add(@year(@client_expire()), "1900")</code>

<code>@set("variable", "value")</code>	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: <pre>@set("month", @xlate_month("Jan", "Feb", "Mar", "Apr", "May", "Jun", "Jul", "Aug", "Sep", "Oct", "Nov", "Dec", @month(@client_expire())))</pre> Variables are global.
<code>@get("variable")</code>	Returns the value of a variable. For example: <ul style="list-style-type: none"> • expire (e.g., <code>@get("expire")</code>)—Returns the client's reauthentication time, in seconds. If there is no reauthentication time specified, it returns a negative number. • my_mac (e.g., <code>@get("my_mac")</code>)—Returns the client's MAC address • pwininput (e.g., <code>@get("pwininput")</code>)—Returns the string that was typed in the password input field • logo (e.g., <code>@get("logo")</code>)—Returns the path to the default (HP ProCurve) logo or the logo uploaded in the Logo field under the Settings tab of the New or Edit Logon Customization page.
<code>@gt("param1", "param2")</code>	Returns true if Param1 is greater than Param2.
<code>@if()</code>	Conditional execution depends on the truth value of the argument to <code>@if()</code> .
<code>@elif()</code>	Zero or more <code>@elif()</code> 's may be followed by zero or one <code>@else()</code> .
<code>@else()</code>	
<code>@endif()</code>	<code>@endif()</code> is always required.
<code>@equal("arg1", "arg2")</code>	Returns 1 if the arguments are identical, 0 otherwise.
<code>@lt("arg1", "arg2")</code>	Returns 1 if arg1 is less than arg2, 0 otherwise.
<code>@gt("arg1", "arg2")</code>	Returns 1 if arg1 is greater than arg2, 0 otherwise.
<code>@le("arg1", "arg2")</code>	Returns 1 if arg1 is greater than arg2, 0 otherwise.
<code>@ge("arg1", "arg2")</code>	Returns 1 if arg1 is greater than arg2, 0 otherwise.
<code>@not("arg")</code>	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. It provides three standard buttons, the Logon User, Logon as a Guest and Logoff buttons.

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>
  <br>
  
</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="/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="#103173"><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>

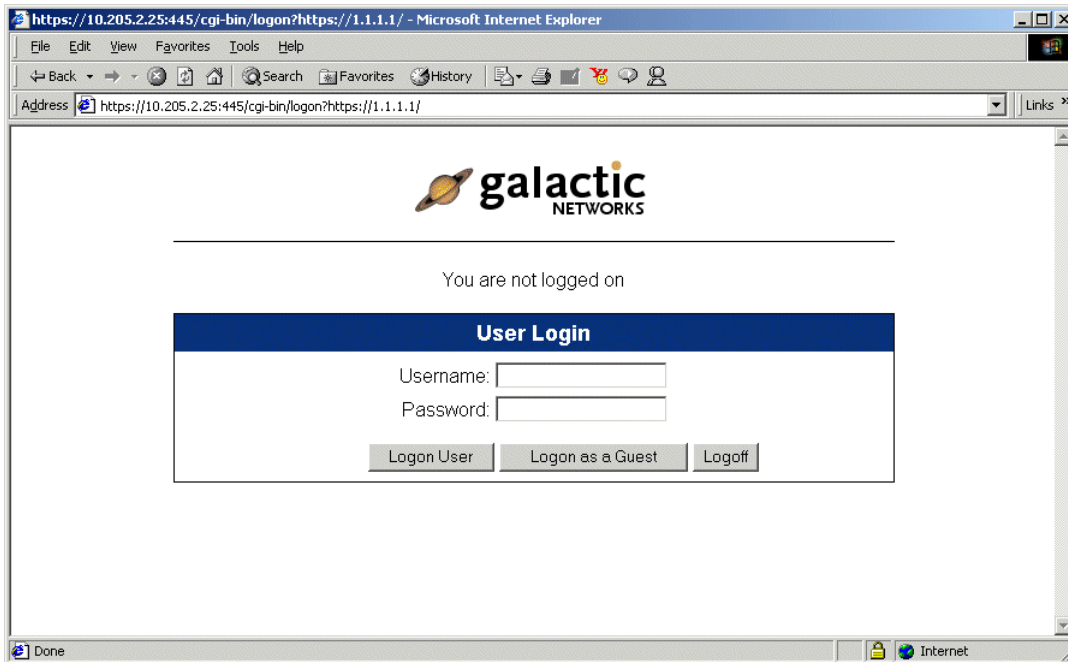
<!-- Displays three buttons -->

      <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 C-2.

Figure C-2. Three-button logon page



Changing the Logon Button Names

If you want to change the names that appear on the buttons on the Logon page, 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=submit value="Visitor Logon">  
<INPUT name=logon_action type=hidden value="Logon as a Guest">
```

If you want to change the button names of more than one button on a single page, each pair of statements must appear within in a separate FORM specification, and each form must include the set of required macros as defined in "Required Macros" on page C-4.

Example 3 shows how you must implement the template if you want to have three buttons that perform the same functions as shown in Figure C-2 (the Logon User, Logon as a Guest, and Logoff buttons) but you want to rename all three. The example is not a complete template, but just shows the parts that provide the renamed buttons.

Example 3

```
<FORM action="/cgi-bin/logon" method=post name=logonForm> (This is the FORM statement  
required at the beginning of the Logon form.)
```

```
    @satmac()  
    @interface()  
    @java_works()  
    @secret()  
    @query()
```

(Not shown -- Code here to set up a table, present username and password input fields etc. >

The following replaces the "Displays three buttons" section in Example 2.

```
<!-- Displays three buttons -->
```

```
    <tr><td align="center">  
        <table>  
            <tr><td align="right" width="200">  
                <INPUT name=logon_action type=submit value="Registered User">  
                <INPUT name=logon_action type=hidden value="Logon User">  
            </FORM> (This is the end of the original FORM statement. The first renamed button can  
                be included within this FORM)  
        </td>
```

```
        <FORM action="/cgi-bin/logon" method=post name=guestForm>  
            @satmac()  
            @interface() (This form enables renaming the second button.)  
            @java_works()  
            @secret()  
            @query()  
            <td align="center" width="100">  
                <INPUT name=logon_action type=submit value="Visitor Logon">  
                <INPUT name=logon_action type=hidden value="Logon as a Guest">  
            </FORM>  
        </td>
```

```
        <FORM action="/cgi-bin/logon" method=post name=logoffForm>  
            @satmac()  
            @interface() (This form enables renaming the third button.)  
            @java_works()  
            @secret()  
            @query()  
            <td align="left" width="100">  
                <INPUT name=logon_action type=submit value="Log me off">  
                <INPUT name=logon_action type=hidden value=Logoff>  
            </FORM>  
        </td>
```

```
    </tr>  
    </table>  
</td></tr>
```

Customizing the Logon Page Messages

There are a number of informational messages that may appear on the Logon page in certain circumstances. These messages may appear in the following circumstances:

- After the client has clicked the logoff button, but before a new logon page appears, a logoff transition message may be displayed. The default version of this message is:
Logging off...
If the logon page does not reappear, click [here](#).
- If the user does not log on within a certain timeframe, the Logon page expires, and the following message appears:
The previous logon page has expired. Click [here](#) for a new logon page.
- If the user attempts to logon too many times with an invalid username or password, the following message appears:
Too many failed logon attempts from this computer. You will be redirected when you are allowed to try again. If <nn> seconds elapse and you're not redirected, click [here](#).
<nn> is the number of seconds the user is forced to wait before a new logon attempt is allowed. This number increases each time the failed logon message is displayed, if the user continues to attempt to logon with invalid credentials.

Each of these messages is produced by a separate page template; you can create custom versions of these templates to provide your own messages.

The only necessary element on any of these pages is a link to the URL page. You obtain the URL page link by using a `@get("l_url")` template function which returns the logon page URL.

```
<a href="@get("l_url")">Your click here message</a>
```

Other than this statement, these pages may include any HTML statements and images you want.

For the "Too many logon attempts..." page, you can also present to the user the number of seconds he or she must wait before attempting to logon again. This value can be obtained using the template function `@get("delta")`. The function returns the number of seconds that must elapse before the user can attempt to logon again (this value is shown as <nn> in the default message shown above). Use of this function is optional.

Once you have created your custom pages, you upload them through the Custom Templates tab of the New or Edit Logon Customization page. The custom pages should be entered into the fields under this tab as follows:

- To change the "Logging off..." message, upload a custom template through the **Logoff Transition Page** field.
- To change the "... logon page has expired..." message, upload a custom template through the **Logon Page Expired Page** field.
- To change the "Too many failed logon attempts..." message, upload a custom template through the **Too Many Attempts Page** field.

Guest Registration Template

To configure a location to allow custom guest registration, there are three elements that must be in place:

- Your main custom logon page must have a “Register as Guest” button instead of the “Logon as a Guest” button. This requires using “Register” instead of “Logon as a Guest” for the “value” attribute of the INPUT specification.
- The **Require guests to register before logging on** option must be selected on the Settings tab of the New or Edit Logon Customization page (accessed from the Logon Customization tab under Rights). If this is not selected, the Guest Registration page will not be displayed.
- A guest registration template may be added through the Custom Templates tab of the New or Edit Logon Customization 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 built-in database. The data from any other fields will appear in the log file entry for the logon event.

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:

Form Tag:

```
<FORM action=/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 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/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. It 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 C-3.

Example 4

```
<!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>
    <br>
    
  </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="/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="#103173"><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>
    </td>
  </tr>
  </table>
  </td>
  </tr>
  </table>
```

```

<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>

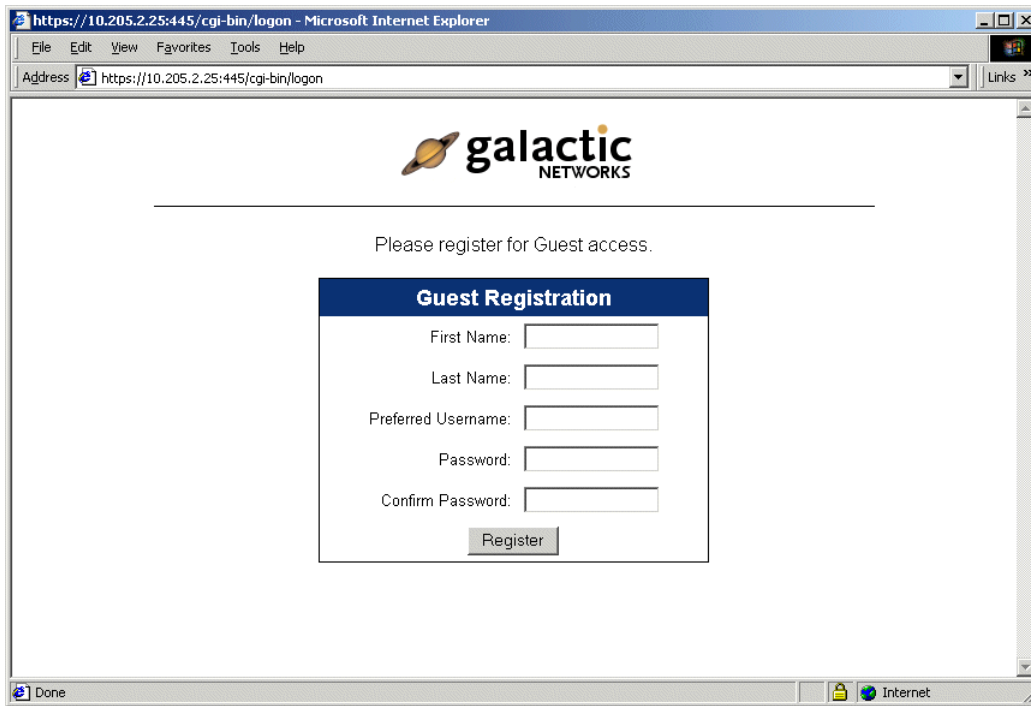
<tr>
  <td align="right"><font size="2"> Confirm Password:</font></td>
  <td align="left"><INPUT type="password" name="confirm" size=15 />
</td>
</tr>

<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 C-3.

Figure C-3. Guest Registration page produced by the template in Example 4



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 Custom Templates tab of the New or Edit Logon Customization page, there are two other steps required to enable the Logoff pop-up feature:

- Step 1.** Enable the logoff pop-up capability by checking the **Display logoff window after logging on** option in the LogonPage section under the Settings tab of the New or Edit Logon 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 C-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 HP ProCurve Logoff pop-up page if you do not provide a customized Logoff page template.

The required elements in a Logoff Pop-up template are:

Form Tag:

```
<FORM action=/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 5

```
<!-- 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>
    <br>
    
</center>
<font face="arial, helvetica, sans-serif">

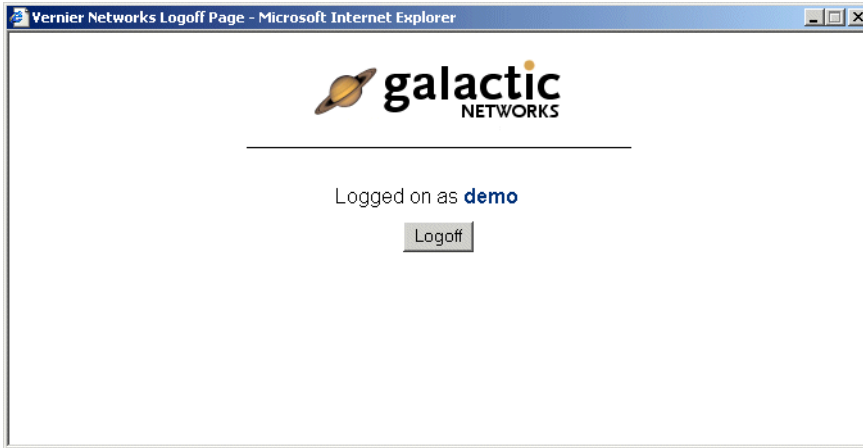
    <FORM action=/logon method=post name=logoffForm>

        <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 C-4.

Figure C-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

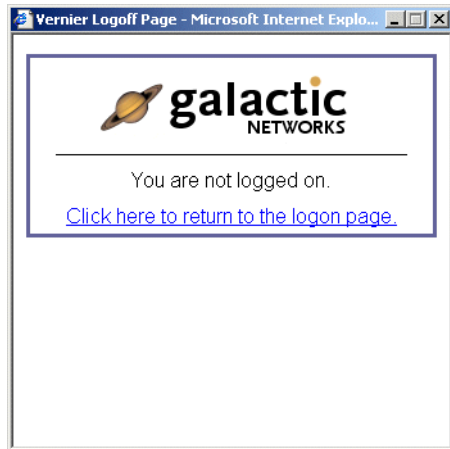
The default 700wl Series-provided Logoff pop-up does not immediately display the Logon page; instead it displays a link that lets the user choose to go to the Logon page. The Logon page is displayed in a separate, fully-functional browser window.

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, then when you click the **Logoff** button the Logoff window changes to display content as shown in Figure C-5:

Figure C-5. Logoff confirmation window



When you click the link, in this window, a fresh Logon page opens in a new window.

To customize this logoff confirmation window, you can upload a custom template in the **Logged Off Window** field under the Custom Templates tab of the New or Edit Logon Customization page.

The only required element on this page is a link to the logon page with the target specified as a new browser window:

```
<a href="@get("l_url")" target="_blank">Your message about link to logon page</a>
```

Other than this statement, the page may include any HTML statements and images of your choosing.

Customizing the Stop Page

Like the Logon, Logoff and Guest Registration pages, the Stop page can also be customized through a custom template file. Because a Stop page does not require any buttons or input fields, there are no required elements for the page. It may consist only of HTML statements of your choosing. However, template functions may be used for retrieving the user name or displaying a user's expiration time. See the functions under "Client Functions" and "Miscellaneous Functions" beginning on page C-6.

TROUBLESHOOTING

This appendix presents troubleshooting procedures for the 700wl Series system. Table D-1 shows the symptoms, probable cause and recommended actions for a variety of problems.

The following are problems you may encounter when configuring your 700wl Series system components for network connectivity and communication.

Table D-1. System Configuration Troubleshooting Guide

Symptom(s)	Probable Cause	Recommended Action
Access Control Server inaccessible from management system after configuration	Incorrect configuration	Access system through Command line Interface (CLI). 1. Check that IP address is correct. 2. If hostname is used, check that it is correctly configured in DNS with both forward and reverse lookup.
	Incorrect network configuration	1. Check default router. 2. Check DNS server configuration 3. Check subnet mask 4. Check configuration of unit to use DHCP or static ip address.
	If all else fails	1. Reboot using command line interface. 2. Restart management system 3. Restore to factory defaults and start over
Can't get to Access Control Server	Incorrect administrator logon name or password	1. Check configuration, particularly passwords 2. Use CLI to reset passwords
NT Domain logon not working	1. 700wl Series system cannot "sniff" logon success 2. Username or password not valid on domain	1. Verify NT Domain Logon selected in Authentication Policy 2. Clients not being NAT'ed (Access Policy NAT set to "When Necessary") 3. External DHCP server configured to provide real IP addresses for clients 2. Kerberos and SMB Allowed Traffic filters enabled in Access Policy.

Table D-1. System Configuration Troubleshooting Guide (Continued)

Symptom(s)	Probable Cause	Recommended Action
RADIUS Authentication not working	<ol style="list-style-type: none"> 1. RADIUS configuration incorrect 2. User name or password not valid 	<p>Test client authentication using Transaction Tracer (under Rights > Authentication Policies> Tools and Options)</p> <ol style="list-style-type: none"> 1. Verify RADIUS service selected in appropriate Authentication Policy 2. Check RADIUS server IP address 3. Check RADIUS “secret” matches on unit and Radius server 4. Ensure correct RADIUS port used (factory default is 1812)
LDAP Authentication not working	<ol style="list-style-type: none"> 1. LDAP configuration incorrect 2. User name or password not valid 	<p>Test client authentication using Transaction Tracer (under Rights > Authentication Policies> Tools and Options)</p> <ol style="list-style-type: none"> 1. LDAP service selected in appropriate Authentication Policy 2. Check LDAP IP address or server port (factory default is 389) 3. Bind setting (user vs. non-user binding) supported for your LDAP implementation 4. Verify the DN, field names, or search strings
No traffic through access point	No connection	<ol style="list-style-type: none"> 1. Check cabling to access point. 2. Use cross-over cable if required 3. Check power to Access Point
	Access point requires server for WEP Key	
	Access Point requires configuration	<ol style="list-style-type: none"> 1. Add MAC address of AP to built-in database as Network Equipment 2. Include AP in Access Points Identity Profile
Client Problems		
No initial web page	Access Controller sees no web request	Use a browser to request http://1.1.1.1
	Browser problems	<p>SSL does not work properly in certain browser versions:</p> <ul style="list-style-type: none"> • Internet Explorer 5.01 with DLL schannel.dll version 4.86.1959.1877 • Certain downrev versions of MAC OS/X browsers

Table D-1. System Configuration Troubleshooting Guide (Continued)

Symptom(s)	Probable Cause	Recommended Action
Client has incorrect access rights	Rights misconfigured	For a connected client, view Client detailed status from the Status > Client Status page. For a non-connected client, use the Simulate User Rights function (under Rights > Authentication Policies> Tools and Options) 1. Verify client is associated with the correct Connection Profile and Identity Profile 2. Verify that the Access Policy provides the rights that you expect.

Error Conditions in the Administrative Console

The following are common conditions or error messages that may appear in the 700w1 Series system Administrative Console.

Table D-2. Administrative Console errors

Error Message(s) or Condition	Cause/Meaning	Recommended Action
Client Status page: the Idle Time for a client is displayed as a negative value	The time settings on the Access Controller and the Access Control Server are not synchronized.	Use the Date & Time function in the Network configuration area to set the date and time of the Access Control Server and Access Controller to be the same, and use NTP to keep them in sync.

GLOSSARY



The glossary defines terms that are used throughout the 700wl Series system. Some of the following terms are in common usage but may have 700wl Series system-specific meanings. These terms are defined in context in the chapter where they first appear.

Term	Definition
802.11	See “IEEE 802.11” on page E-5
802.11a	See “IEEE 802.11a” on page E-5
802.11b	See “IEEE 802.11b” on page E-5
802.11g	See “IEEE 802.11g” on page E-5
802.1x	See “IEEE 802.1x” on page E-5
802.3af	See “IEEE 802.3af” on page E-5
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 Point (AP)	A wireless hardware device that attaches to a wired network and transmits data to and receives data from your wireless network cards or adapters. Sometimes called a Base Station.
Access Points Identity Profile	An Identity Profile that contains only MAC addresses that are Access Points. This may be associated with an Access Policy for the Access Points connected to the system through one or more Access Controllers.
Access Policy	<p>A specification in the 700wl Series system Rights Manager that specifies what access is allowed. Specifically the Access Policy consists of:</p> <ul style="list-style-type: none">• IP Addressing and VLAN settings• Encryption protocols and authentication methods• The set of filters that identify client packets that are permitted to be passed by the Access Controller (Allows” and filters that identify and change the destination of client packets (Redirects).• HTTP filters• Bandwidth usage filters• Timeout settings <p>Access Policy were defined as a set of Allows and Redirects in previous versions of the 700wl Series system.</p>

Term	Definition
AH	<p>Authentication Header protocol. AH digitally signs the entire contents of each packet, protecting your network against three kinds of attacks:</p> <p><i>Replay attacks</i>, where an attacker captures packets, saves them until later, and resends them. These attacks may allow an attacker to impersonate a machine after that machine's no longer on the network. The AH protocol prevents replay attacks by including a keyed hash of the packet, so no one else can resend the packets.</p> <p><i>Tampering</i>. IPSec's keyed hash mechanism provide assurance that no one has changed the contents of a packet after it was sent.</p> <p><i>Spoofing</i>. The IPSec AH protocol provides two-way authentication, so the client and server can both verify the other end's identity.</p>
Allowed Traffic filters	Filters that identify client packets that are permitted to be passed by the Access Controller.
ARP	Address Resolution Protocol - A protocol for mapping an IP address to a physical machine address that is recognized in the local network.
Authentication	A means of proving that a client is who it claims to be through use of a password or shared secret.
Authentication Policy	A named, ordered set of authentication services used to perform user logon authentication for a set of clients. This was called authentication realm in previous versions of the 700wl Series system.
Authentication service	A single instance of a service used for authentication, such as a specific Active Directory service, or specific RADIUS server.
bridge	Bridges (like switches) are devices that control the transmission of data at the link layer, which controls data flow, handles transmission errors, provides physical (as opposed to logical) addressing. Examples of popular link layer protocols include Ethernet, Token Ring, and FDDI.
broadband wireless	Wireless transmission at high speed. Wireless transmission is slower than wire-line speeds; thus, whereas land-based broadband generally starts at T1 rates, wireless might be considered broadband starting at 250kbps.
CA	Certificate Authority - A known organization, such as Verisign, that issues digital certificates. A digital certificate is an electronic ID that establishes your credentials in transactions on the Web.
CAST	An encryption algorithm that allows for a range of key sizes. CAST is one of the encryption algorithms supported by 700wl Series system.
CHAP	Challenge Handshake Authentication Protocol (CHAP) is a widely-supported authentication method in which the knowledge of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends the remote access client a challenge string. The remote access client uses the challenge string and the user's password, and computes a Message Digest-5 (MD5) hash. The MD5 hash is sent to the remote access server. The remote access server, who has access to the user's password, performs the same hash calculation and compares the result with the hash sent by the client. If they match, the remote access client's credentials are considered authentic.

Term	Definition
CLI	Command Line Interface: 700wl Series system Access Controllers, Integrated Access Managers, and Access Control Servers all have a command line interface through which they can be controlled, as an alternate to using the Administrative Console.
Client	A machine, device, or user of the 700wl Series system.
CMAK	Connection Manager Administration Kit - This is a tool provided by Microsoft to allow you to customize the Microsoft Connection Manager.
Community String	The protocol password for SNMP
Connection Profile	A named set of an Authentication Policy, VLAN tag policy, a set of Locations and a set of Time Windows that specify how users can connect to the 700wl Series system.
Access Control Server	A logical device that performs two functions: <ul style="list-style-type: none"> 1) Coordinates between the Access Controllers and the Rights Manager 2) Coordinates Access Controller-to-Access Controller communications, such as a roaming handoff.
cookie	See <i>session cookie</i> .
CSR	Certificate Signing Request - A CSR is a text file generated by a Web server which contains Information about your organization and your Web or WAP Server's public key. A CA will use the CSR to generate your signed digital certificate, which is required to initialize an SSL session.
DAP	Directory Access Protocol - DAP is part of X.500, a standard for directory services in a network.
datagrams	A datagram is a packet format defined by IP. An IP datagram has a header that is made up of five or six 32-bit words, followed by data. The header includes two length fields, one that specifies the length of the header and one that specifies the entire length of the packet. The terms datagram and packet are often used interchangeably.
DHCP	Dynamic Host Configuration Protocol - A protocol that assigns a dynamic IP address to a device on a network. This dynamically assigned IP address is granted on a "lease" or temporary basis. Once a lease expires on a device, the next time that device attempts to connect to the network, a new IP address may or may not be assigned. Dynamic Host Configuration Protocol -DHCP allows a computer to join an IP-based network without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, releases and renews these addresses as devices leave and re-join the network. <i>Cf.</i> NAT
Diffie-Hellman	A key agreement protocol (also called exponential key agreement) developed by Diffie and Hellman in 1976. The protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. Diffie-Hellman protocol allows for the derivation of a shared secret value (that is, key) from one party's public key and another party's private key.
DN	Distinguished Name. In an LDAP service the every entry has a primary key called the Distinguished Name (DN).

Term	Definition
DNS	Domain Name Server - A DNS translates Internet domain names such as xyzcorp.com, into IP addresses.
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.
DSA	Directory System Agent - In X.500, each local directory is called a Directory System Agent (DSA). A DSA can represent one organization or a group of organizations. The DSAs are interconnected from the Directory Information Tree.
EAP	Extensible Authentication Protocol (EAP) is an extension to the Point-to-Point Protocol (PPP) that allows arbitrary authentication methods using credential and information exchanges of arbitrary lengths. EAP provides an industry-standard architecture for support of additional authentication methods within PPP.
ESP	A part of IPSec: Encapsulated Security Payload (Provides encryption plus authentication. The main use for IPSec)
Ethernet	An industry-standard network hardware specification (802.3) developed by IEEE that offers dedicated network (and Internet) access.
Everywhere	A Location that includes all Access Controllers (and thus all ports) managed by the 700wl Series system. Until you create another Location, this is the location to which <i>all</i> clients are associated.
Expire time	A timer that determines how long before a user must re-authenticate.
Firewall	A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. All messages entering or leaving the private network pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
FQDN	Fully Qualified Domain Name: A complete domain name consisting of a host, the second-level domain, and the top-level domain. For example, www.xyzcorp.com is a FQDN. www is the host; xyzcorp is the second-level domain; and .com is the top level domain.
Gateway	A hardware or software device that provides access to the Internet for multiple computers or networks. Sometimes called a gateway router.
Guest user	A client who matches the Guest Identity Profile, and is granted Guest access based on the Access Policy associated with the Guest Identity Profile. Clients who click the Guest button on the logon page become members of this Identity Profile.
Host	Used in Sabre (in HTTP Filters) to refer to protocols (www, ftp)? a node that users (people) use to access the Internet (?)
HTML	Hyper Text Markup Language - HTML is the authoring language used to create documents on the World Wide Web.
HTTP	Hyper Text Transfer Protocol - HTTP is the underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

Term	Definition
HTTP Proxy	An Web server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes: improving performance and filtering requests.
Hub	A piece of hardware that contains a series of ports (usually 4, 8, or 16), which allow you to network your computers or extend an existing network. Hubs broadcast packets to all of its ports, but only the computer meant to receive the packet accepts it.
ICMP	Internet Control Message Protocol - ICMP is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user. The ICMP is formally described in the Internet Engineering Task Force's RFC 792.
Identity Profile	A named set of user or network equipment grouped together for purposes of sharing the same Connection Profile or Access Policy Identity Profiles were called groups in previous versions of the 700wl Series system.
IEEE	Institute of Electrical and Electronics Engineers - A professional organization that develops standards for the computer industry, including the commonly used IEEE 802.11b wireless networking standard.
IEEE 802.11	A family of specifications for wireless networking, first published in 1997 by IEEE. The original specification allows for speeds up to 2 Mbps and operates in the 2.4-GHz frequency range using both frequency hopping and direct sequence spread spectrum technologies.
IEEE 802.11a	One specification for wireless networking, ratified in 1999 by IEEE. 802.11a operates in the 5-GHz frequency range and uses OFDM (orthogonal frequency division multiplexing) technology. 802.11a allows for speeds up to 54 Mbps.
IEEE 802.11b	The most commonly used standard for wireless networking, ratified in 1999 by IEEE. 802.11b, also known Wi-Fi, operates in the 2.4-GHz frequency range and uses direct sequence spread spectrum technology. 802.11b allows for speeds up to 11 Mbps.
IEEE 802.11g	The latest specification for wireless networking from IEEE, still under development. 802.11g operates in the 2.5-GHz frequency range and uses OFDM (Orthogonal Frequency Division Multiplexing) technology. 802.11g allows for speeds up to 54 Mbps.
IEEE 802.1x	IEEE 802.1x is a protocol for port-based authentication. It structures authentication as a process between three logical entities: a requester, an authenticator, and an authentication server.
IEEE 802.3af	IEEE standard 802.3af-2003 defines the specifications to deliver power over standard Ethernet cables. The standard was approved by the IEEE Standards Board on June 12, 2003
IGMP	Internet Group Management Protocol - An Internet protocol that provides a way for an Internet computer to report its multicast group membership to adjacent routers. IGMP is formally described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2236.

Term	Definition
IKE	A part of IPSec: IKE=Internet Key Exchange (Negotiates session parameters for the authentication header and ESP. Sets up Security Associations (SA))
Inner Tunnel Address	For a connection using PPTP or L2TP, the IP address associated with the actual data from the client, encapsulated within the outer tunnel. The inner tunnel address may be NAT'ed, but NAT is not required.
Integrated Access Manager	A unit that combines the Access Control Server and Rights Manager with an Access Controller.
IP	<p>Internet Protocol - The established standard protocol for transmitting and receiving data in packets over the Internet. IP is a fundamental part of the TCP/IP protocol.</p> <p>Internet Protocol; the <i>IP</i> part of the <i>TCP/IP</i> communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or subnetwork. IP accepts "packets" from the layer 4 transport protocol (TCP or UDP), adds its own header to it, and delivers a "datagram" to the layer 2 data link protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.</p>
IPSec	<p>Internet Protocol Security: A protocol for negotiating encryption and authentication at the IP (host-to-host) level. SSL secures only one application socket; SSH secures only a login; PGP secures only a specified file or message. IPsec encrypts everything between two hosts.</p> <p>IPSec = AH + ESP + IPcomp + IKE, where AH = Authentication Header (Provides a packet level authentication service); ESP = Encapsulated Security Payload (Provides encryption plus authentication. The main use for IPSec); IPcomp = IP payload compression (to compress packets before encryption); IKE=Internet Key Exchange (Negotiates session parameters for the authentication header and ESP. Sets up Security Associations (SA))</p> <p>IPSec provides computer-level authentication, as well as data encryption, for VPN connections that use the L2TP protocol. IPSec negotiates between your computer and its remote tunnel server before an L2TP connection is established, which secures both passwords and data.</p> <p>L2TP uses standard PPP-based authentication protocols, such as EAP, MS-CHAP, CHAP, SPAP, and PAP with IPSec.</p>
IrDA	A standard, created by the Infrared Data Association, for wireless, infrared transmission systems between computers.
IrDA port	A transmitter/receiver for infrared signals.
ITU	International Telecommunications Union
JavaScript	A scripting language to enable Web authors to create client-side, interactive web pages. Although it shares some features and structures with the Java language, it is independent of Java.
Kerberos	Kerberos is a secure method for authenticating a request for a service on a computer network. Kerberos lets a user request an encrypted "ticket" from an authentication server; this ticket can then be used to request a particular service. The advantage of Kerberos is that the user's password does not have to go through the network.
KDC	Key Distribution Center: A network service that supplies session tickets and temporary session keys used in the Kerberos V5 authentication protocol.

Term	Definition
L2F	Layer 2 Forwarding; a tunneling protocol from Cisco
L2TP	Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used to enable a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP and L2F.
LDAP	Lightweight Directory Access Protocol - LDAP is software protocol for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate intranet. LDAP is a lightweight version of Directory Access Protocol (DAP), which is part of X.500.
Linger timeout	A timer that controls how long before a client must re-authenticate after being disassociated from an Access Controller.
Location	A named set of Access Controllers or Access Controller ports that are used to define a Connection Profile.
MAC	Media Access Control - Specific protocols that govern network device access to a network.
MAC address	a unique identifier for each physical network device, used by MAC to identify the network device
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 database of managed objects accessed by network management protocols. An SNMP MIB is a set of parameters which an SNMP manager can query or set in the SNMP agent of a network device (e.g. router). In theory, any SNMP manager can talk to any SNMP agent with a properly defined MIB.
MAP	Micro Access Point
MPPE	Microsoft Point to Point Encryption
MSCHAP	Microsoft Challenge Authentication Protocol
NAP	Network Access Point.
NAS	Network Access Server
Network Address Translation (NAT)	Network Address Translation: NAT is a technique for translating one set of IP addresses, often private, to another set, often public. This provides a means of creating a private IP address space for 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).
Network Equipment	Equipment such as Access Points that connects to the 700wl Series system. Network equipment is identified by its MAC address
NMS	Network Management System: SNMP software systems for managing networks, for example, HP OpenView, CA Unicenter, Concord NetHealth, etc.
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).
NTP	Network Time Protocol—a protocol used to synchronize computer clock times in a network of computers

Term	Definition
Outer Tunnel Address	The IP address associated with a PPTP or L2TP connection within which the client traffic is encapsulated. This address will always be a NAT'ed address, regardless of the group NAT settings.
Packet	A piece of data transmitted over a network that includes not only data, but also a header in which the intended address of the packet is listed. Depending on the protocol, additional information may be included in the packet's layers.
Packet filters	Determine what client traffic an Access Controller will allow onto the network based on the client's rights.
Port Address Translation (PAT)	in conjunction with NAT, provides a private IP address space to a set of devices. PAT rewrites the source port number before forwarding packets on to the network.
PPP	PPP (Point-to-Point Protocol) is a protocol for communication between two computers using a serial interface. It is sometimes considered a member of the TCP/IP suite of protocols. PPP provides layer 2 (data-link layer) service.
PPTP	Point-to-Point Tunneling Protocol - An encryption protocol and technology for creating Virtual Private Networks (VPNs). PPTP is used to ensure that messages transmitted from one VPN node to another are secure.
Proxy Server	See HTTP Proxy.
PuTTY	An SSH client for use with Microsoft Windows
RADIUS	Remote Authentication Dial-In User Service; RADIUS is commonly used to provide centralized authentication, authorization and accounting for dial-up, virtual private network and wireless network connections. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share.
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	<i>Obsolete term</i> See Authentication Realm
Redirected Traffic filters	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. The ability to move out of the range of a one access point into the range of another access point while staying connected to the network.
Router	A hardware device that connects networked computers or LANs. A router determines which route (or path) a packet takes during transmission to its destination. Home networking routers can also act as firewalls or gateways.
Service	See Authentication service.
session cookie	A session cookie, is a small file that contains information about a user that disappears when the user's browser is closed. Unlike a persistent cookie, a session cookie is not stored on your hard drive but is only stored in temporary memory that is erased when the browser is closed. Session cookies are used to enable the 700wl Series system Access Control Server (or Integrated Server) to be able to track the screens that a user has visited during a session so that information can be customized for the user. SSL is used to encrypt the information contained in the cookie.

Term	Definition
Session redirectors	Client TCP and UDP sessions can be redirected from their original destination IP address or port.
SNMP	Simple Network Management Protocol - The network management protocol of most modern TCP/IP-based networks. SNMP monitors the activity of various devices on a network.
SOAP	Simple Object Access Protocol - SOAP is designed to solve the problem of passing live objects over the network. SOAP structures its messages into headers and payloads. The payload can be any valid XML structure. In other words, SOAP is a general XML message passing system.
SSH	Secure SHell - SSH is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. When using SSH's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.
SSL	Secure Socket Layer: The SSL protocol is the web standard for encrypting communications between users and web sites, to prevents eavesdropping and tampering with any transmitted data.
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. <i>cf.</i> DHCP, NAT
Subnet	A subnet (short for "subnetwork") is an identifiably separate part of an organization's network. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network (LAN). Having an organization's network divided into subnets allows it to be connected to the Internet with a single shared network address.
Subnet mask	Once a packet has arrived at a gateway or connection point with its unique network number, it can be routed using the subnet number as well. The router knows which bits to look at (and which not to look at) by looking at a subnet mask. A mask is simply a screen of numbers that indicates which subnet bits are relevant. Using a mask saves the router having to handle the entire 32 bit address; it can simply look at the bits selected by the mask.
Switch	A more intelligent (and expensive) hub that routes data to the computer meant to receive it. A regular (passive) hub broadcasts packets to all of its ports where only the computer meant to receive the packet accepts it. Broadcasting has a lower throughput than routing.
TCP/IP	Transmission Control Protocol/Internet Protocol - An industry-standard protocol that determines the way packets of data are formatted, transmitted and received between networks. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. UDP is an alternate transport that does not guarantee delivery. IP provides the routing mechanism. TCP/IP is a routable protocol, which means that all messages contain not only the address of the destination station, but the address of a destination network. Every client and server in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at startup.

Term	Definition
tcpdump	A program that prints out the headers of packets on a network interface that match a specified filtering criteria. The syntax used by tcpdump is used 700wl Series system for specifying packet filters.
TFTP	Trivial File Transfer Protocol - A lightweight version of FTP
Time Window	A time windows is defined in the 700wl Series system Rights Manager as a range of hours, dates, or days of the week. These may be used when defining Connection Profiles to limit the connection profile to a specified time period.
trusted device	A device that has been authenticated.
UDP	<p>User Datagram Protocol - UDP is a lightweight transport built on top of IP. UDP squeezes extra performance from IP by not implementing some of the features a more heavyweight protocol like TCP offers. Specifically, UDP allows individual packets to be dropped (with no retries) and UDP packets to be received in a different order than they were sent.</p> <p>UDP is often used in videoconferencing applications or games where optimal performance is preferred over guaranteed message delivery. UDP is one of the oldest network protocols, introduced in 1980 in RFC document 768.</p>
Uplink port	The Ethernet 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.
URI	A Uniform Resource Identifier is a formatted string that serves as an identifier for a resource, typically on the Internet. URIs are used in HTML to identify the anchors of hyperlinks. URIs in common practice include Uniform Resource Locators (URLs) and Relative URLs
URL	Uniform resource locator; the address that defines the route to a file on the Web or any other Internet facility. URLs are typed into the browser to access Web pages, and URLs are embedded within the pages themselves to provide the hypertext links to other pages.
VLAN	Virtual Local Area Network - A logical grouping of two or more computers, which are not necessarily on the same physical network segment, given priority access privileges across the LAN backbone in order to provide the same network behavior they would receive if they were connected to the same physical segment.
Wireless Data Privacy	The ability to encrypt all client traffic using standard encryption technology such as PPTP, L2TP, and IPsec.
VPN	<p>Virtual Private Network - A VPN is one or more WAN links over a shared public network, typically over the Internet or an IP backbone from a Network Service Provider (NSP), that simulates the behavior of dedicated WAN links over leased lines.</p> <p>Virtual Private Network. A network which uses the public network to transfer information using secure methods. For example, you could set up a VPN between your home office and your business office using security and encryption and the Internet as your transfer pipe.</p> <p>A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.</p>
WAP	Wireless Application Protocol; determines how wireless devices utilize internet content and other services.

Term	Definition
Web server	Network host that acts as an HTTP server; a computer that provides World Wide Web services on the Internet; it includes the hardware, operating system, Web server software, TCP/IP protocols, and the Web site content (Web pages).
WEP	Wired Equivalent Privacy - WEP is a common, but not very secure, way of protecting wireless networks and part of the Wi-Fi specification's built-in encryption scheme. Known to be vulnerable.
Wi-Fi	Wireless Fidelity - The standard used by wireless component manufacturers to make their products compatible with other wireless products. The IEEE 802.11b wireless standard is also known as Wi-Fi.
WINS	Windows Internet Naming Service - WINS is a MS Windows system for determining the IP address associated with a particular network computer. DNS is an alternative system for name resolution suitable for network computers with fixed IP addresses.
WLAN	<p>Wireless Local Area Network - A derivative of a traditional LAN that uses radio waves to transmit data rather than cables.</p> <p>Wireless LAN; a local area network that transmits over the air typically in an unlicensed frequency such as the 2.4GHz band. A wireless LAN does not require lining up devices for line-of-sight transmission like IrDA. Wireless access points (base stations) are connected to an Ethernet hub or server and transmit a radio frequency over an area of several hundred to a thousand feet and can penetrate walls and other nonmetal barriers. Roaming users can be handed off from one access point to another like a cellular phone system. Laptops use wireless modems that plug into an existing Ethernet port or that are self contained on PC cards, while standalone desktops and servers use plug-in cards (ISA, PCI, and so on).</p>
WLIF	Wireless LAN Interoperability Forum; a membership group that endorses products that are interoperable with major standards; supports OpenAir and 802.11.
X.500	<p>X.500 Directory Service is a standard way to develop an electronic directory of people in an organization so that it can be part of a global directory available to anyone in the world with Internet access. The idea is to be able to look up people in a user-friendly way by name, department, or organization. Because these directories are organized as part of a single global directory, you can search for hundreds of thousands of people from a single place on the World Wide Web.</p> <p>In X.500, each local directory is called a Directory System Agent (DSA). A DSA can represent one organization or a group of organizations. The DSAs are interconnected from the Directory Information Tree (DIT). The user interface program for access to one or more DSAs is a Directory User Agent (DUA). DUAs include whois, finger, and programs that offer a graphical user interface. X.500 is implemented as part of the Distributed Computing Environment (DCE) in its Global Directory Service (GDS).</p>
XML	Extensible Markup Language. An open standard for describing data from the W3C. It is used for defining data elements on a Web page and business-to-business documents. It uses a similar tag structure as HTML; however, whereas HTML defines how elements are displayed, XML defines what those elements contain. HTML uses predefined tags, but XML allows tags to be defined by the developer of the page.

Term

XML-RPC

Definition

XML-RPC is designed to be a simple procedural way for a client program to make function requests of another program. It provides similar functionality to SOAP, but is more limited and, generally, much simpler to use. The 700w Series system supports the use of XML-RPC as an authentication service.

INDEX OF COMMANDS

A

add snmpmanager <hostname> <ip-address> [/<mask>]	A-35
add snmptrapreceiver <ip-address>	A-36

C

cancel backup	A-26
cancel upgrade	A-28
clear accesscontrolserver	A-14
clear admin	A-4
clear dhcpserver	A-10
clear dns	A-11
clear domainname	A-9
clear gateway	A-10
clear hostname	A-9
clear ipsecsecret	A-22
clear logs	A-31
clear natdhcp	A-18
clear ntpserver	A-33
clear portmedia <port> <slot>/<port>	A-13
clear sharedsecret	A-11
clear snmpcommunity	A-36
clear snmpcontact	A-36
clear snmplocation	A-35
clear snmpport	A-35
clear syslogserver	A-17
clear upgradeproxy	A-29
clear wins	A-12
cli AC ACS	A-4
create backup	A-25

D

debug interface [<slot>/<port>]	A-32
debug ip [<slot>/<port>]	A-32
debug tcpport <tcp port> [<slot>/<port>]	A-32
delete networkadmin <login>	A-5

delete policyadmin <login>	A-5
delete snmpmanager all <hostname> <ip-address> [/<mask>]	A-35
delete snmptrapreceiver all <ip-address>	A-36
delete superadmin <login>	A-5
disable redundancy	A-16

E

enable redundancy	A-16
exit	A-4

F

factoryreset	A-30
--------------------	------

G

get backup <url>	A-26
get upgrade <url> <key> [reboot version mindowngrade]	A-27

H

help [diag help ipsec snmp]	A-3
---	-----

L

logoff client {all mac < mac-address> }	A-25
---	------

N

nslookup <hostname>	A-31
---------------------------	------

P

ping {<ip-address> <hostname>}	A-32
--	------

R

reboot [upgrade downgrade same]	A-29
refresh client all [mac <mac-address>]	A-8
remote cancel <ip-address>	A-18
remote datetime <ip-address> <date> <time>	A-19
remote factoryreset <ip-address>	A-20
remote ping <ip-address>	A-18
remote reboot <ip-address>	A-20
remote rebootalt <ip>	A-20
remote shutdown <ip-address>	A-20
remote sysinfo <ip-address> [<item>]	A-19
remote upgrade <ip-address> <url> <key>	A-20

remote upgradecheck <ip-address> <url>	A-21
remote upgradereboot <ip-address> <url> <key>	A-21
remote upgradestatus <ip-address>	A-21
restore backup.	A-26

S

set accesscontrolserver <ip-address>	A-14
set admin <login-name> [<password> <password>].	A-4
set datetime <date> <time>.	A-34
set dhcp on off	A-10
set dhcpserver <ip-address>	A-10
set dns <primary-ip-address> [<secondary-ip-address>]	A-11
set domainname <domainname>	A-9
set espencryption [des] [3des] [blowfish] [cast] [aes] [none]	A-22
set espintegrity [md5] [sha1] [none]	A-22
set gateway <ip-address>	A-10
set hostname <hostname>	A-9
set ikedh [group1] [group2] [group5]	A-22
set ikeencryption [des] [3des] [blowfish] [cast]	A-22
set ikeintegrity [md5] [sha1].	A-22
set initialcontact on off	A-22
set ip { <ip-address> [<netmask>] <ip-address>/<maskbits> }	A-9
set ipsec on off	A-22
set ipsecsecret [<secret> <secret>].	A-22
set l2tp on off.	A-22
set natdhcp <ip-address> <subnetmask> [<lease-time> [<time-units>]]	A-18
set networkadmin pass enable disable <login>.	A-5
set ntp on off	A-34
set ntpserver{< ip-address> <hostname>} [<ip-address> <hostname>]	A-33
set policyadmin pass enable disable <login>	A-5
set portmedia {<port> <slot>/<port>} " <media> [<media-option>] "	A-13
set pptp on off	A-22
set redundancy [peer <peer ip-address>] [priority <priority value>] [retry <retry time>] [failover <failover time>]	A-16
set remote on off	A-6
set sharedsecret [<secret> <secret>]	A-11
set snmp on off	A-35
set snmpauthtraps on off.	A-36
set snmpcommunity <community>	A-36
set snmpcontact <contact>	A-35
set snmplocation <location>	A-35
set snmpport <port>	A-35
set ssh on off	A-22
set sshcli on off	A-6
set superadmin pass enable disable <login>	A-5

set syslogserver <ip-address> [<facility>]	A-17
set timezone <general-tz> <specific-tz>	A-33
set upgradeproxy [on off] [host <ip-address> [<port>]] [user <user> [<password>]]	A-29
set uplink [<slot>/<port>]	A-12
set wins <primary-ip-address> [<secondary-ip-address>].	A-11
show ac [mac <mac-address>]	A-16
show accesscontrolserver	A-14
show admin	A-4
show backup	A-27
show bridging.	A-15
show client mac <mac> [rights]	A-24
show clientprobes	A-15
show clients [<filter>] [sort <sort>] [reverse]	A-23
show clients [mac <mac-address>] [sort {mac ip user machine port sessions idle}] [reverse]	A-24
show deviceport <device>	A-8
show dhcpserver	A-10
show ether [status].	A-7
show forwardipbroadcasts	A-15
show id.	A-7
show ip.	A-10
show logs [<severity>] [max <lines>] [for <count> <time-units>] [search <quoted-text>] [reverse].	A-30
show natdhcp.	A-18
show networkadmin [<login>]	A-5
show policyadmin [<login>]	A-6
show portip	A-14
show portmedia <port> <slot>/<port>	A-13
show product	A-8
show redundancy.	A-17
show remote	A-6
show serial.	A-8
show sharedsecret.	A-11
show slots	A-7
show snmp.	A-36
show sshcli	A-6
show status	A-6
show superadmin [<login>]	A-5
show syslogserver	A-17
show time.	A-34
show upgrade	A-28
show upgradeproxy	A-29
show uplink	A-12
show version	A-8
show vpn	A-23
shutdown	A-29
store backup <url> [<filename>]	A-26

T

traceroute {<ip-address > | <hostname>} [<hops> [<probes> [<probewait>]]]. A-32

INDEX

Numerics

802.1Q VLAN tag	
specifying in Access Policy	4-46
specifying in Connection Profile	4-33
802.1x	
configuring as authentication service	5-16
configuring RADIUS for	5-17
monitored logon	5-3
802.2 protocol	6-24
802.3 protocol	6-24

A

Access Control Server	
changing administrator username/password	6-5
configuring	6-3
configuring redundant peer	6-6
deleting a redundant peer	6-7
DHCP Network for NAT Clients	6-23
editing the configuration	6-3
enable technical support access	6-5
enabling SSH CLI access	6-5
new installation default configuration	2-1
shared secret	6-5
Access Control Server redundancy	
avoiding data loss	2-19
configuring	6-15
disabling redundancy	6-17
how failover works	2-18
requirements	6-15
system configuration for	6-15
Access Controller	
configuration via CLI	A-14
configuring NAS-ID for accounting	6-12
deleting from System Components List	6-13
enable technical support access	6-12
enabling SSH CLI access	6-12
new installation default configuration	2-2
selecting a folder	6-12
troubleshooting	D-2
Access Points	
adding to built-in database as network	
equipment	4-22
and Identity Profiles	4-3

in built-in database	4-20
troubleshooting	D-2
Access Policies	4-39
802.1Q VLAN tags in	4-46
Allowed Traffic tab	4-49
Bandwidth tab	4-58
example of modification	4-79
HTTP Proxy tab	4-55
overview of	4-4
predefined	4-40
Redirected Traffic tab	4-52
specifying encryption	4-46
the Settings tab	4-45
the Timeout tab	4-59
access rights	
configuring, overview of	4-5
how they are assigned	4-7
overview of	4-1 to 4-6
simulating for a user	5-42
view user rights	3-11
accounting	
RADIUS accounting	5-20
active client management commands	A-23
Active Directory service	5-13
address variables	
creating user-defined variable	4-71
in Allowed or Redirected Traffic filters	4-70
predefined address variables	4-70
addressing	
and VLANs	2-26
in the 700w1 Series system, overview of	2-21
Administrative Console	
common buttons and icons	2-15
Header bar	2-7
Navigation Bar	2-7
Navigation bar	2-8
navigation buttons	2-8
summary of functions	2-9
System Components List	2-11
tabs and sub-tabs	2-10
working with tables	2-13
administrator	
changing on Access Control Server	6-5
changing username/password	2-5

changing username/password on Integrated Access Manager	6-10	monitored logon	5-3
changing username/password on Integrated System	6-12	NT Domain logon	1-3, 5-3
default name and password	2-4	tracing authentication transactions	5-47
logging in as	2-4	using 802.1x	5-16
logging out	2-6	using a Kerberos service	5-17
troubleshooting incorrect password	D-1	using a RADIUS service	5-19
Advanced Setup tab	6-21	using an LDAP service	5-9
DHCP Network for NAT Clients	6-23	using an XML-RPC service	5-22
aliasing		using iPlanet directory service	5-14
in LDAP to get user information	5-15	wireless data privacy logon	5-3
Allowed Traffic filters	4-4	authentication logging	
AC HTTPS Logon page	4-51	enabling	9-5
AC Logon-forward no URI	4-51	Authentication Policies	
AC Logon-fwd append URI	4-51	creating or editing	5-6
AC SSL Stop page	4-51	defined	5-2
AC Stop page	4-51	deleting	5-5
All IP Traffic	4-51	predefined System Authentication Policy	5-4
and bridging	6-25	preferred for Connection Profiles checkbox	5-6
AppleTalk	4-51	replacing the default policy	5-6
CDP and WNMP	4-51	Authentication Realm	<i>See</i> Authentication Policies
DHCP	4-51	Authentication Service	
DNS TCP	4-51	configuring	5-7 to 5-29
DNS UDP	4-51	configuring 802.1x	5-16
example-the Outside World filter	4-82	configuring a RADIUS service	5-19
External CS UI	4-51	configuring Active Directory	5-13
filter list	4-62	configuring an LDAP service	5-9
Grid view	4-41	configuring Kerberos	5-17
HTTP	4-51	configuring XML-RPC	5-22
Internal Admin UI	4-51	defined	5-2
Internal HTTP	4-51	editing from Authentication Policies page	5-5
Internal IS UI	4-51	auto refresh settings	2-12
Internal rights UI	4-52	automatic HTTP proxy	6-26
IP Fragments	4-52		
Kerberos filter	4-52	B	
Outside World	4-52	backing up the Access Control Server	8-13
Ping	4-52	backup and restore commands	A-25
predefined filters	4-51	bandwidth management	
SMB UDP	4-52	overview	2-20
SMBTCP	4-52	rate limiting per user	4-59
tcpdump expression in	4-65	Bandwidth tab	4-58
Allowed Traffic tab	4-49	basic configuration tasks	2-16
allows, <i>See</i> Allowed Traffic filters		bridging	6-24
alternate version software		and Allowed Traffic filters	6-25
restarting with	8-12	AppleTalk traffic	6-24
AppleTalk protocol	6-24	CDP traffic	6-24
ARP request		enabling/disabling	6-24
client polling	6-25	IPX/802.2	6-24
Audience	3-ix	IPX/802.3	6-24
authenticate call response	5-25	IPX/Ethernet II encapsulation	6-24
authenticate methodCall (XML-RPC)	5-22, 5-24	Layer 2 packets	6-24
authentication	1-3	SLC protocol	6-24
802.1x logon	1-3, 5-3	WNMP traffic	6-24
browser-based	1-3, 5-2	broadcasts	
external group identity retrieval	5-28	configuring ports for	6-26
		enabling	6-26

browser-based logon	1-3, 5-2	overview of	4-3
Built-in authentication service	5-2	the Locations tab	4-33
built-in database	4-16	the Settings tab	4-32
adding Access Points	4-22	the Time Windows tab	4-34
adding users	4-17	custom logon pages	5-30
network equipment	4-21	creating or editing	5-32
retrieving MAC addresses from external		custom template files	5-40
LDAP service	4-24	customizing text	5-34
users	4-16	customizing the logo	5-33
C		guest registration	5-30
CDP bridge traffic	6-24	logo image types	5-34
centralized management and administration	2-3, 2-17	logoff page pop-up	5-37
Certificate Authority	7-7	small browser support (PDAs)	5-33
Certificate Signing Request		Stop image types	5-38
CSR	6-30	stop page	5-37
certificated-based IKE authentication	7-5	uploading images for	5-40
Cisco Discovery Protocol	6-24	custom templates	
client addressing		Guest Registration page	5-40
using dynamic IP addressing (DHCP)	2-21	Logoff page	5-40
using NAT mode	2-21	Logon page	5-40
using static IP	2-21	Stop page	5-40
Client Detail page	3-9	uploading images for	5-40
client polling	6-25	D	
ARP request	6-25	date and time	
configuring	6-26	configuring	6-40
polling interval	6-26	using NTP server	6-41
time-out counter	6-26	deleting	
client status		Access Controller	6-13
filtering display	3-9	redundant peer Access Control Server	6-7
clients		DHCP	
disassociating	6-25	/30 setting	6-23
Command Line		and port subnetting	6-36
Access Controller configuration commands		external DHCP server for client addressing	
A-14		6-20	
active client management	A-23	Full subnet setting	6-23
backup and restore commands	A-25	getting component IP address via	6-20
Help	A-3	Lease Time	6-23
network configuration	A-9	Netmask for NAT	6-23
SNMP configuration commands	A-34	network setting for NAT	6-23
status commands	A-6	DHCP Network for NAT Clients	6-23
stopping and restarting the system	A-29	disassociating a client	6-25
system access commands	A-4	display filters	2-12, 3-13
upgrading system software commands	A-27	DNS filter pairs	4-72
Command Line Interface	A-1	creating or editing a filter pair	4-73
accessing	A-2	filters list	4-72
command syntax	A-3	Document Conventions	3-ix
for an Integrated Access Manager	A-2	domain name	
configuring		in network configuration	6-20
Access Control Server	6-3	Dynamic IP mode	
Integrated Access Manager	6-7	for client addressing	2-21
Connection Profiles	4-29	E	
802.1Q VLAN tags	4-29	encryption	
creating or editing	4-31	specified in Access Policy	4-46

Ethernet bridging, enabling	6-24	Stop image types	5-38
Expire timer, <i>See</i> reauthentication timeout		uploading for custom templates	5-40
export rights	5-50	importing rights	5-52
External	4-51	inaccessible Access Control Server,	
external identity retrieval	5-28	troubleshooting	D-1
F		incorrect network configuration, troubleshooting	D-1
Failover <i>See</i> Access Control Server redundancy		incorrect rights, troubleshooting	D-3
filters		Integrated Access Manager	
display filters	2-12	changing administrator username/password	6-10
folders		configuring	6-7
creating or editing	6-13	configuring NAS-ID for accounting	6-10
selecting for an Access Controller	6-12	editing the configuration	6-8
vs. Locations	6-14	enable technical support access	6-10
Full DHCP Subnet setting	6-23	enabling SSH CLI access	6-10
G		shared secret	6-10
getMemberList methodCall (XML-RPC)	5-24	Integrated System	
Guest user		changing administrator username/password	6-12
Guest Registration page custom template	5-40	interfaces	
logon options	5-34	port connection type	6-34
registered guest option	5-35	speed/duplex settings	6-34
guest user		Subnet tab	6-37
registered guest	5-30	Interfaces tab	6-34
Guest users		IP address	
pre-registering	4-16	setting for Access Controller ports	6-36
H		IP broadcasting	
Header bar	2-7	configuring ports for	6-26
Help		enabling	6-26
for Administrative Console	2-5	iPlanet directory service	
for CLI	A-3	configuring as authentication service	5-14
hostname		IPSec	
in network configuration	6-20	and authentication	5-3
HTTP proxy		certificate configuration	7-5
automatic	6-26	configuring	7-2
server configuration	6-26	configuring PKI for	7-5
HTTP Proxy filters	4-4, 4-75	shared secret	7-4
creating or editing a filter	4-76	IPX/802.2 protocol	6-24
example	4-83	IPX/802.3 protocol	6-24
proxy filter types	4-77	IPX/Ethernet II encapsulation protocol	6-24
Verify via DNS option	4-78	K	
HTTP Proxy tab	4-55	Kerberos	5-2
I		configuring as authentication service	5-17
Identity Profiles	4-11	Kerberos realm	5-18
and NT Domain logon	5-28	Key Distribution Center	5-18
creating or editing	4-13	L	
overview of	4-3	L2TP/IPSec	
predefined profiles	4-12	and authentication	5-3
Idle time		Layer 2 bridging	6-24
in session status display	3-13	layer 3 roaming	1-4
images		layer 3 roaming, overview	2-23
logo image types	5-34		

LDAP service			
authentication troubleshooting	D-2	adding to built-in database	4-19
configuring for authentication	5-9	how rights are assigned	4-8
configuring MAC address retrieval	4-26	Identity Profile default	4-3
non-user binding	5-10	Management Information Base (MIB)	6-38
retrieving MAC address users from	4-24	Maximum Concurrent Logons per User	4-14
user binding	5-10	maximum packet size	4-52
using aliasing to get user information	5-15	monitored logon	1-3, 5-3
License Information		N	
viewing	3-15	NAS-ID	5-21
Lightweight Directory Access Protocol (LDAP)	5-2	configuring on Access Controller	6-12
Linger timeout	2-23, 4-59	configuring on Integrated Access Manager	6-10
and client polling	6-25	NAT mode	
configuring start	6-26	for client addressing	2-21
Locations	4-4, 4-35	NAT <i>See</i> Network Address Translation	
creating or editing	4-36	Navigation Bar	2-7
Locations tab	4-33	Network Address Translation (NAT)	1-5, 4-47
logo		and roaming support	2-24
customizing on Logon page	5-33	and VPN tunneling	2-23, 4-48, 7-12
uploading images	5-40	DHCP setting for	6-23
Logoff page		overview of	2-21
custom template	5-40	setting in Access Policy	4-45
pop-up option	5-37	network configuration	6-17, A-9
Logon page		domain name	6-20
administrator logon	2-4	external DHCP server	6-20
custom template	5-40	getting IP address via DHCP	6-20
Logon as Guest option	5-34	hostname	6-20
registered guest option	5-35	SSL certificate and hostname	6-20
logon page customization	5-30	using static IP address	6-20
creating or editing a custom pages	5-32	network equipment	4-4
custom template files	5-40	adding a device to built-in database	4-22
customizing text	5-34	in built-in database	4-21
customizing the logo	5-33	network setup	6-17
guest registration	5-30	Advanced Setup tab	6-21
logo image types	5-34	Basic Setup tab	6-19
logoff page pop-up	5-37	Interfaces tab	6-34
small browser support (PDAs)	5-33	SNMP tab	6-38
Stop image types	5-38	Subnet tab	6-36
stop page	5-37	time zone configuration	6-41
Logs		Time&Date tab	6-40
enabling authentication logging	9-5	non-user binding for LDAP	5-10
enabling session logging	9-5	NT Domain logon	5-27
session log entry format	9-6	Allowed Traffic filters for	5-27
viewing	9-1	and Identity Profiles	5-28
		and Network Address Translation	5-27
M		monitored logon	5-3
MAC address		troubleshooting	D-1
and Identity Profile	4-3	NTP server	
in session status display	3-13	configuring	6-41
MAC address retrieval		O	
configuring LDAP search parameters	4-26	Online Help, using	2-5
from external LDAP service	4-24	OpenSSL	6-31
getting group identity information	4-28		
MAC address spoofing detection	6-23		
MAC address user			

P			
password			
changing for administrator	2-5		
troubleshooting	D-1		
PDAs			
logon page options	5-33		
peer Access Control Server			
configuring peer name	6-6		
deleting	6-7		
PKI			
configuring for IPSec	7-5		
PKI certificates			
generating	7-5		
polling			
ARP request	6-25		
clients	6-25		
Port Address Translation (PAT)	2-21		
ports			
advanced network configuration	6-36		
configuring for valid IP addresses	6-36		
configuring IP broadcasting for	6-26		
port subnetting	6-36		
Reserved port	6-36		
setting connection type	6-34		
speed/duplex settings	6-34		
subnets and DHCP	6-36		
post-authentication group identity retrieval	5-28		
PPTP			
and authentication	5-3		
predefined filters			
Allowed Traffic filters	4-51		
Redirected Traffic filters	4-54		
Preferred Primary Control Server setting	6-6		
Protocol			
in session status display	3-13		
R			
RADIUS			
authentication troubleshooting	D-2		
configuring as authentication service	5-19		
configuring for 802.1x authentication	5-17		
RADIUS accounting	5-20		
accounting data	5-21		
configuring the NAS-ID	6-10, 6-12		
enabling	5-20		
NAS-ID	5-21		
Start packet contents	5-21		
Stop packet contents	5-21		
rate limiting, bandwidth	4-59		
Real IP mode			
for client addressing	2-21		
overview	2-21		
Realms <i>See</i> Authentication Policies			
reauthentication timeout	4-59		
Redirected Traffic filters	4-4		
		AC HTTP Logon	4-54
		AC HTTPS Logon	4-54
		AC Internal blocker	4-54
		AC Logon page shortcut	4-54
		AC No SSL Web	4-54
		AC No Web	4-54
		ACS-to-AC Logon	4-54
		ACS-to-AC Stop	4-54
		Blackhole	4-54
		creating or editing a filter	4-67
		filters list	4-66
		Grid view	4-42
		No external rights UI	4-54
		No internal admin UI	4-54
		No internal IAM UI	4-55
		No internal rights UI	4-55
		No SSL internal UI	4-55
		predefined filters	4-54
		SOCKS	4-55
		tcpdump expression in	4-69
		Redirected Traffic tab	4-52
		redirects, <i>See</i> Redirected Traffic filters	
		redundant Access Control Servers	
		configuring	6-15
		registered guest	4-16, 5-30
		logon page option	5-35
		pre-registering	4-20
		Remote Authentication Dial-in User Service (RADIUS)	5-2
		Remote Profiles API	5-24
		Reserved port	6-36
		Rights	
		configuring, overview	4-5
		how they are assigned	4-7
		simulating for a user	5-42
		view user rights	3-11
		Rights Assignment Table	4-6
		creating a new row	4-10
		editing a row	4-11
		rights configuration	
		exporting	5-50
		import from a file	5-52
		Rights Manager	
		overview of	4-4
		Rights Table	4-7
		roaming	1-4, 2-23
S			
		secondary Access Control Server	
		function limitations	6-16
		Serial console	A-2
		exiting	A-2
		session logging	
		enabling	9-5
		Syslog facility	9-5

syslog server, configuring	9-5	stopping and restarting the system through CLI	
Session Logs		A-29	
log entry format	9-6	subnets	
viewing	9-6	configuring per Access Controller port	6-36
session status		Syslog facility	
filtering display	3-13	for session logging	9-5
Settings tab		Syslog server	9-6
in a Connection Profile	4-32	for session logging	9-5
in Access Policy	4-45	system access commands	A-4
shared secret	6-7, 6-10	System Authentication Policy	5-4
configuring on Access Control Server	6-5	System Components List	2-11, 6-2
for IPSec	7-4	deleting an Access Controller	6-13
for RADIUS	5-20	System Components page	6-2
SLC protocol	6-24		
small browser logon page option	5-33		
SNMP		T	
configuration via CLI	A-34	tcpdump expression	4-65, 4-69
configuring	6-38	example	4-82
enabling /disabling	6-38	technical support access	
management console configuration	6-40	enabling on Access Controller	6-12
MIB support	6-38	enabling on an Access Control Server	6-5
monitoring via network management		enabling on Integrated Access Manager	6-10
application	6-38	time and date	
setting Community name	6-39	configuring	6-40
trap events	6-40	using NTP server	6-41
trap receiver configuration	6-39	Time Windows	4-4, 4-37
SNMP tab	6-38	creating or editing	4-38
Speed/Duplex tab	6-34	Time Windows tab	4-34
spoofing detection	6-23	time zone configuration	6-41
SSH		Time&Date tab	6-40
and authentication	5-3	Timeout tab	4-59
SSH command line access		transaction tracer	5-47
enabling on Access Control Server	6-5	trap receivers (SNMP)	
enabling on Access Controller	6-12	configuring	6-39
enabling on Integrated Access Manager	6-10	troubleshooting	
SSL certificate		inaccessible Access Control Server	D-1
unknown certificate warnings	6-20	incorrect administrator password	D-1
static IP address		incorrect network configuration	D-1
configuring 700wl Series component using	6-20	incorrect rights	D-3
static IP mode			
for client addressing	2-21	U	
Status	3-1	update software	8-2
Access Controller	3-5	upgrading system software	8-2
Access Controller, detailed	3-5	through CLI	A-27
Client	3-7	uploading images	
client, detail	3-9	for custom logon templates	5-40
Equipment	3-3	user binding for LDAP	5-10
Session	3-12	user profile, for XML-RPC	5-22
status commands	A-6	User Rights Simulator	5-42
status displays		user-defined address variables	4-71
auto refresh setting	2-12	users	4-4
display filters	2-12	adding to built-in database	4-17
Stop page		in built-in database	4-16
custom template	5-40		
customizing	5-37		

V

Verify via DNS	
HTTP proxy filter option	4-78
Virtual LANs (VLANs)	1-6, 2-24
and IP addressing	2-26
and the 700wl system, overview	2-24
specifying tag in Access Policy	4-46
specifying tag in Connection Profile	4-33
VLAN tags in Connection Profiles	4-29
VPN tunneling	
and Network Address Translation	2-23

W

warranty	1-ii
Whens <i>See</i> Time Windows	
Wheres <i>See</i> Locations	
WINS filter pairs	4-72
creating or editing a filter pair	4-73
filters list	4-72
Wired Equivalent Privacy	7-1
wireless data privacy	
overview of	1-4
supported protocols	5-3
wireless data privacy logon	5-3
Wireless Network Access Protocol	6-24
WNMP bridged traffic	6-24

X

XML-RPC service	5-24
authentication and authorization using	5-22
external, for authentication	5-22
user profile	5-22
XML-RPC-based service	5-2



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

June 2004

Manual Part Number
5990-8809

