Introduction to
Software Version 4

HP ProCurve
Secure Access
700wl Series

www.hp.com/go/hpprocurve

HP PROCURVE
SECURE ACCESS 700WL SERIES

INTRODUCTION TO SOFTWARE
VERSION 4

Publication Number

5990-8807
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

This preface describes the audience, use, and organization of the *Introduction to Software Version 4* manual. It also outlines the document conventions, safety advisories, compliance information, related documentation, support information, and revision history.

Document Objectives

The guide instructs you in how to:

- Understand the new rights model for 700wl Series system, version 4
- Navigate easily through the pages of the new Administrative Console to perform standard tasks

Audience

The audience for this document are network administrators who currently use HP ProCurve products running software version 3.1, and who have been tasked with upgrading those systems to use version 4 software. This document assumes a high degree of familiarity with the 700wl Series system version 3.1 software, and also a high degree of familiarity with the unique rights configuration of the system to be upgraded.

How To Use This Document

This document contains an introduction to the new user interface, workflow, and features implemented in the version 4 software, specifically covering how those features relate to or differ from the features, user interface and workflow of version 3.1.

Document Conventions

The following text conventions are used in this document:

Table 1. Text Conventions

Convention	Definition
Boldface Arial	Page menus that you click to select, commands that you select, or field names are in boldface Arial.
Boldface Italic Palatino	New terms that are introduced are in boldface italic Palatino.

Table 1. Text Conventions

Convention	Definition
Italic Palatino	Emphasized terms are in italic Palatino.
`Courier`	Filenames and text that you type are in `Courier`.

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

Table 2. Notices

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

Organization

This document is organized as follows:

Chapter 1—“Introduction”

This chapter provides an overview of what is new in this release of the 700wl Series system, and how users rights have been changed to make them more intuitive and easier to manage.

Chapter 2—“The New Administrative Console”

This chapter explains the new Administrative Console and shows users familiar with earlier versions of the 700wl Series system where to find existing functionality. After reading this chapter you can use the new Administrative Console. Should you need more assistance with a specific feature of the Administrative Console, you can consult the *Configuration and Users’ Guide*.

Chapter 3—“The New Rights Manager”

This chapter familiarizes you with the new model for user rights in the 700wl Series system. The new rights model is similar to the previous model with which you are familiar, but has been changed to make it more intuitive and easier to manage. There have been some changes in terminology, considerable changes in how you set up and manage rights (to greatly streamline your workflow), and some changes in functionality. Read this section carefully before you start to migrate your current system to the new version. Should you need more assistance with a specific feature of the Administrative Console, you can consult the *Configuration and Users’ Guide*.

Appendix A—"Functionality Changes"

This appendix provides a brief list of what has changed in the latest version:

- Terminology changes
- Functionality changes
- New functionality

Appendix B—"Function Map: Version 3.1 to Version 4"

This appendix is a table that shows users experienced with the old Administrative Console where to find each function in the new Administrative Console. Functions are grouped in the same way they are in the old Administrative Console. Consult this appendix if you need to find where to perform some function you are familiar with in the old Administrative Console.

For Further Information

The 700wl Series system, version 4 comes with the following documents.

Table 3. 700wl Series system Document List

Document Name	Description
HP ProCurve Secure Access 700wl Series Upgrading Software Version 3 to Version 4	This document provides step-by-step instructions for upgrading an existing 3.1 system to version 4 Available in PDF format on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve
HP ProCurve Secure Access 700wl Series Management and Configuration Guide	The main users' guide for 700wl Series system software. This guide is available in both PDF and HTML format from the Help button within the Administrative Console. Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve
HP ProCurve Secure Access 700wl Series Installation and Getting Started Guide *(hardware specific)*	This document explains how to set up the 700wl Series system hardware and perform the initial configuration setup so that the components are in communication. Shipped with each Access Control Server or Integrated Access Manager. Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve
HP ProCurve 700wl Series Quick Start Guide *(hardware specific)*	These guides are for experienced administrators who are comfortable doing the initial out-of-the box system configuration using the command line interface. Shipped with each hardware unit Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve

Table 3. 700wl Series system Document List

Document Name	Description
HP ProCurve Secure Access 700wl Series Wireless Data Privacy Guide	This document describes how to configure clients for a variety of security protocols on client systems. Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve
Release Notes	Release notes are shipped in hardcopy format with the product and are also available on the technical support pages of the HP ProCurve web site at www.hp.com/go/hpprocurve.

1

INTRODUCTION

This guide provides an introduction to HP ProCurve Secure Access 700wl Series version 4 software for administrators familiar with version 3.1. It also provides a brief overview of the steps required to migrate a version 3.1 configuration to version 4. The topics in this chapter are:

What's New in Version 4?

The 700wl Series system software version 4 has a number of significant new features, including:

- A new user interface that provides enhanced usability and improved workflow
- A redesigned rights model that makes configuring authentication and access policy much easier
- Centralized management of the elements of a 700wl Series system
- Support for multiple administrators with different administrative roles
- Support for redundant Access Control Servers and Access Control Server failover
- Client-based bandwidth rate limiting
- Enhanced VLAN support

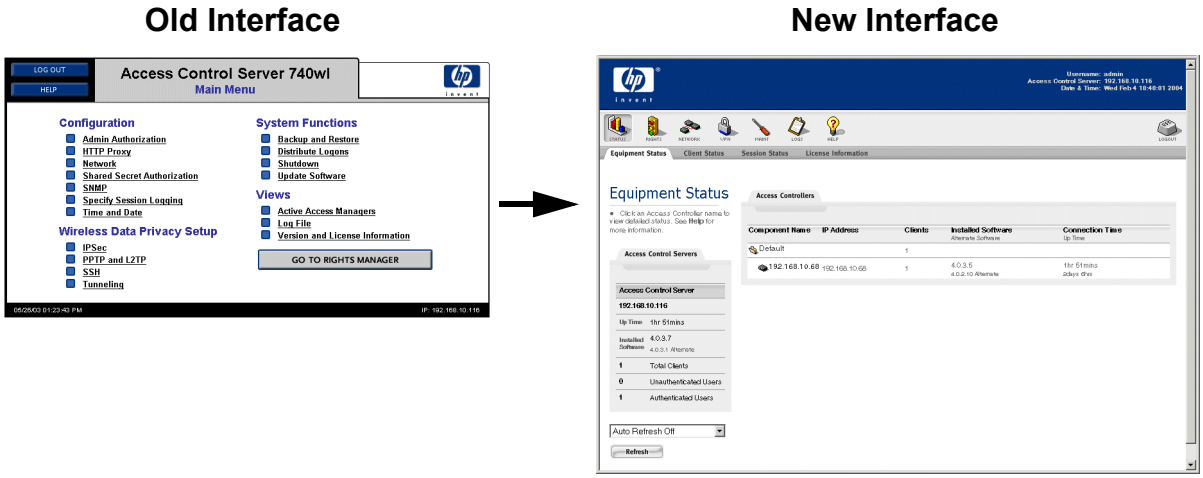
New User Interface

The new user interface is a significant enhancement to the 700wl Series system. Functions are grouped in a more logical manner, workflow has been streamlined for common tasks; and the look and feel of the interface has been redesigned and made more consistent (see Figure 1-1).

The new Administrative Console has been designed based on extensive user experience with the 700wl Series system. It groups features and function together in a more process-oriented way. Common functions are easier to get to and common actions require going to fewer pages of the Administrative Console. For example, defining a "where" with the old Administrative Console takes 23 mouse clicks. With the new Administrative Console the same action (now known as defining a location) can take as few as 7 mouse clicks.

Chapter 2 "The New Administrative Console" surveys the new Administrative Console, showing where the features and functions of the old interface are now located, and briefly explains how to work with the new Administrative Console. After reading Chapter 2, you should be able to find your way around the new user interface to perform the functions familiar to you from version 3.1. The *700wl Series System Management and Configuration Guide* provides a much more in-depth explanation of the features of version 4 of the 700wl Series system.

Figure 1-1. The Old vs. the New Administrative Console



New Rights Model for Authentication and Access

700wl Series system version 4 uses a new rights model that is streamlined, more logical, and much simpler to configure. The underlying concepts are familiar to users of 700wl Series system version 3.1, but the way rights are created and managed has been greatly simplified and terminology has been changed to be clearer.

The 700wl Series system uses a client's *Location* (the Access Controller port through which it is connected), the currently applicable *Time Window*, and optionally, a VLAN tag, to match the client to a *Connection Profile*. The Connection Profile determines the *Authentication Policy* that is used to authenticate the client. The system also uses the client's identity (user name or MAC address) to match the client to an *Identity 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.

Chapter 3, "The New Rights Manager" in this document provides a more detailed overview of the new Rights Management function. The *700wl Series System Management and Configuration Guide* provides a a much more thorough discussion of using the new Rights Management features.

Centralized Configuration and Management

With the new Administrative Console you can configure, monitor and manage all the 700wl Series system equipment from one central Administrative Console accessed from the Access Control Server. Information about Access Controller status and configuration is maintained on the Access Control Server, and is propagated to the Access Controller whenever configuration changes are made. You no longer need to go to the Administrative Console for each Access Controller to update the software, back up the system, or make any other configuration changes; in fact, the browser-based Administrative Console is no longer supported on an Access Controller.

The only configuration functions that *must* be performed on an Access Controller are those that enable the unit to be recognized on the network (setting the unit's IP address, gateway, etc.) and to communicate with the Access Control Server (IP address and shared secret). These few commands are performed through the CLI when the unit is first installed on the network. Once an Access Controller is recognized

by the Access Control Server, all configuration from then on is performed from the Access Control Server's Administrative Console.

Because configuration information for all system components is maintained centrally, centralized management has the following implications:

- The Administrative Console on the Access Controller is no longer accessible through a browser—providing the IP address of an Access Controller will display a page redirecting you to the Access Control Server.
- Only a subset of CLI commands are available on an Access Controller—specifically those that enable network configuration, plus selected status commands. Commands that duplicate configuration functions that should be performed centrally will be disabled.
- Backups are performed for the system as a whole, not individually for each Access Controller.
- All logging is handled centrally. From the Administrative Console you can view the logs from any of the system components.
- Client and session status from all Access Controller is displayed centrally—you can view all clients for the 700wl Series system as a whole (multiple system components) as well as for individual Access Controllers.

Access Control Server Redundancy and Failover

To provide high availability, 700wl Series system version 4 supports paired redundant Access Control Servers. One Access Control Server acts as the primary Access Control Server, managing the 700wl Series system. The other Access Control Server keeps a synchronized copy of the 700wl Series system configuration and database. Should the primary Access Control Server fail, or be unavailable due to a network failure, the secondary Access Control Server takes over. This is transparent to users, who continue to have their proper access and services.

Multiple Administrator Levels

The system administrator can create multiple administrator accounts. Version 4.1 allows three levels of administration, providing needed access to the Administrative Console without having to give all administrators full access.

- *Network Administrators* 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.
- *Policy Administrators* 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.
- *Super Administrators* 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 users.

Client-based Bandwidth Rate Limiting

700wl Series system version 4 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.

Enhanced VLAN Support

700wl Series system version 4 provides enhanced support for VLAN tagging. In version 3.1, VLAN tags were maintained or added to data packets from the client. In version 4, when an Access Controller forwards a DHCP request for a client that is being VLAN tagged going upstream, the Access Controller now tags the DHCP request with the VLAN of the client. This allows you to have port subnets and VLANs with different DHCP servers. In addition, support for VLAN segregation has been added, so that clients in a VLAN only receive packets for that VLAN.

Improved System Logging and Log Analysis

All the system events that are logged are now entered into a unified log database. Instead of having to examining the log file for each Access Controller and for the Access Control Server, all the log information can be found in one place. The log file can be filtered by Access Controller or other criteria as appropriate to aid in monitoring or troubleshooting.

Remote Command Line Interface

Access to the Command Line Interface is now available remotely through an SSH client in addition to being accessible through the serial port. Each 700wl Series system component includes a new setting, **Enable SSH command line interface**, to allow access by this method. All CLI commands are available through this mechanism.

Expanded SNMP Support

700wl Series system version 4 introduces an additional set of Management Information Bases (MIBs) that can provide statistical and state information on the 700wl Series system. Third-party network management systems, such as HP OpenView, CA Unicenter, Concord NetHealth, etc. can query these MIBS via SNMP to provide real-time monitoring and reporting. In addition to the previously supported MIB-II - RFC 1213 and SNMPv2-MIB, version 4 has added:

- New 64-bit counter support for high speed interfaces in IF MIB - RFC 2863
- An HP Systems MIB that provides information on product type, software version, SNMP notifications, and environmental statistics
- An HP-MEMPROC MIB that provides statistics about overall product load (both CPU and memory use)

700wl Series system version 4 has added a new SNMP trap:

- A failover trap—If the secondary Access Control Server becomes the primary Access Control Server (failover) that Access Control Server issues a failover trap.

Upgrading from Version 3.1 to Version 4

Important: *Upgrading from a version 3.1 to version 4 currently requires that you recreate some of your Rights configuration within the new Rights model.*

With previous releases of the 700wl Series system software, each new version was backwards-compatible; after the upgrade, the complete system configuration, including the Rights Manager configuration, was preserved and was still functional. The version 4 software is different in that it is not entirely backwards-compatible. In particular, the Rights Manager configuration is not entirely preserved upon an Access Control Server/Integrated Access Manager upgrade, and your rights configuration must be recreated under the new Rights model.

The basic building blocks—Wheres, Whens, Allows, Redirects, authentication services and the built-in user database—are migrated automatically during the upgrade, but groups, locations and Authentication Realms are not. You must create Identity Profiles, Connection Profiles, Access Policies and Authentication Policies that map the functionality of your 3.1 groups, locations and Authentication Realms.

Upgrade Requirements

HP ProCurve Access Control Server 740wl, Access Controller 720wl, and Integrated Access Manager 760wl units that are running software versions 3.1 can be upgraded to software version 4.

Because the software architecture has changed, you must upgrade ***all*** interconnected units to version 4—in other words, all Access Controllers connected to an Access Control Server or Integrated Access Manager running version 4 must be also upgraded to version 4.

See the *Upgrading HP ProCurve 700wl Series Software Version 3 to Version 4* guide for detailed instructions on upgrading and migrating your 700wl Series system to software version 4.

2

THE NEW ADMINISTRATIVE CONSOLE

This chapter introduces you to the new user interface for the 700wl Series system. It demonstrates how the new Administrative Console differs from the previous user interface and shows you where to find the proper pages for the system tasks you perform. The topics covered in this chapter include:

Note: *When using the new Administrative Console, if you want further information on a particular page, consult the on-line documentation by clicking on the* ***Help*** *button (*  *) to get context-sensitive help for that page.*

In many cases the contents of the new Administrative Console pages are similar to the old pages, so you should be able to use the much of the new interface immediately. The exception is the Rights Manager, which has been redesigned to make it simpler and more intuitive to use. See Chapter 3, "The New Rights Manager" for an explanation of how the new Rights Manager works.

Note: *In Version 4.0 you interact with all the components of the 700wl Series system through one Administrative Console that runs on your Integrated Access Manager or Access Control Server. You no longer need to connect directly to the Administrative Console of an Access Controller to configure, monitor or manage it. All configuration is done centrally from the Integrated Access Manager or Access Control Server Administrative Console. The 700wl Series system automatically propagates changes to the affected Access Controllers as appropriate.*

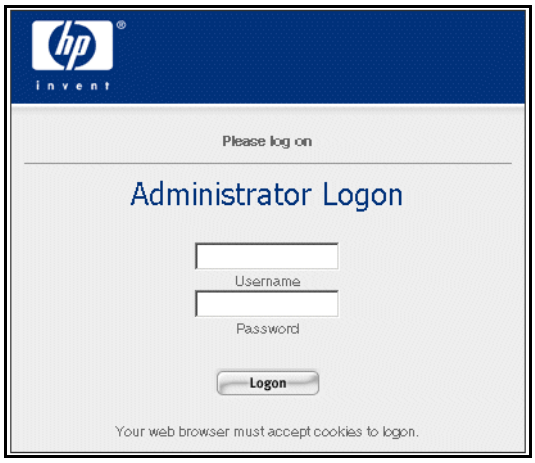
Connecting to the Administrative Console

Logging on to the Administration Interface over the network is the same as for version 3.1:

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

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

Figure 2-1. Administrator Login page



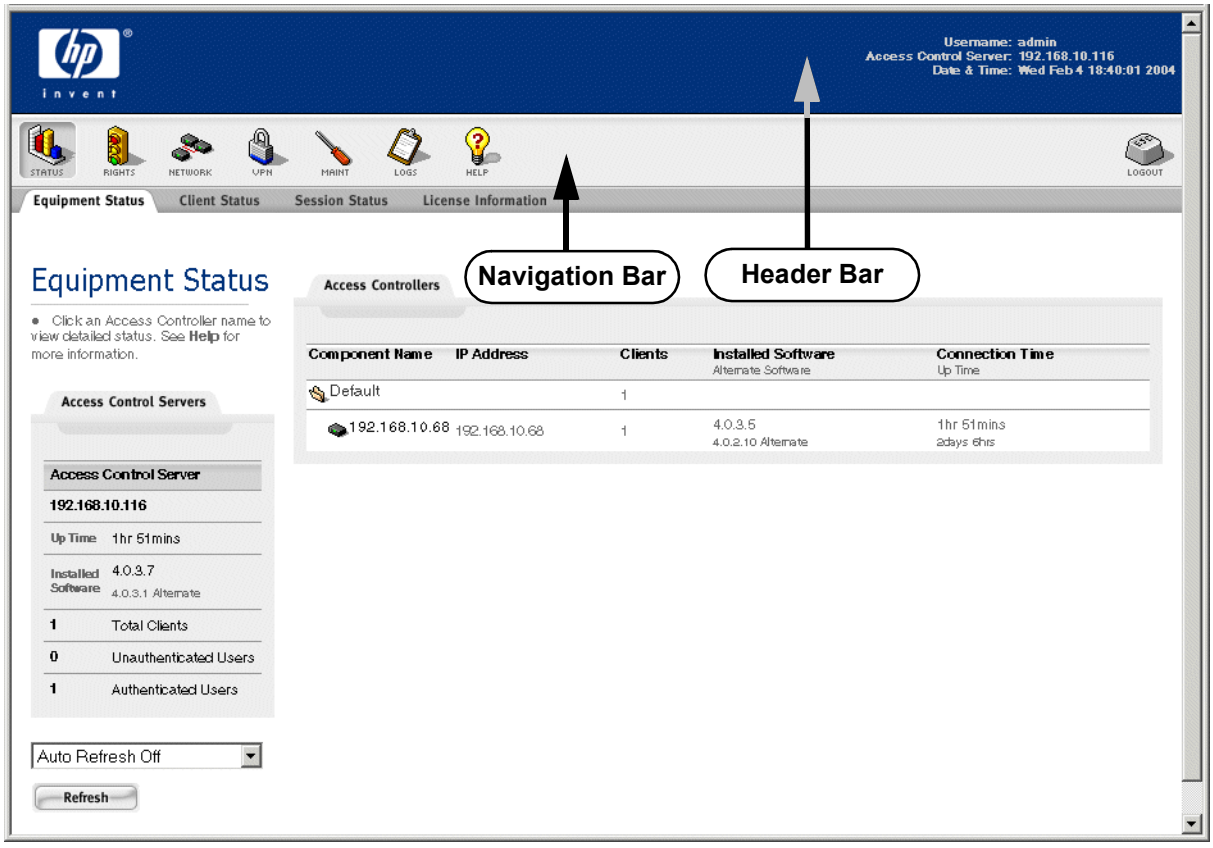
Enter your administrator name and password. The default administrator username is "admin" and the default administrator password is "admin."

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

You should immediately change the administrator password and set the system date, time and time zone.

The initial Administrative Console page shows the status of the components of your system, as shown in Figure 2-2.

Figure 2-2. Initial Administrative Console Page



At the top of the page is the *Header bar* that displays information about this administrative session and the system it is running on, and a *Navigation bar* with icons for each of the main functional areas of the system. To go to one of these functional areas, click the appropriate icon.

To logout of the 700wl Series system, click on the logout button at the far right of the Navigation bar. Figure 2-3 shows the main menu page of the old Administrative Console and where the **Logout** button is now located on the Navigation bar of the new Administrative Console.

Figure 2-3. Where to find the Help and Logout buttons

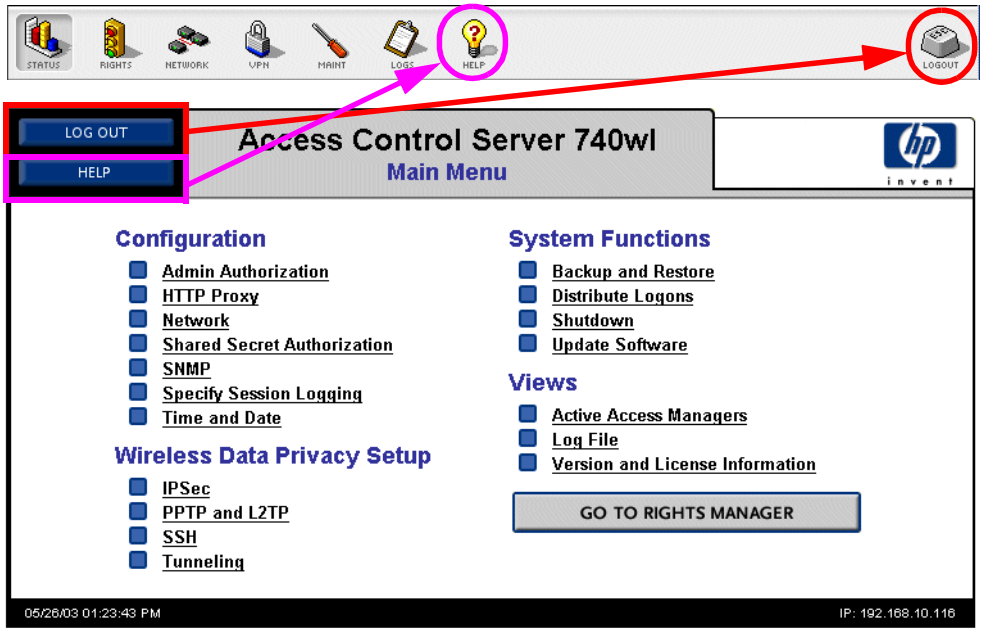


Figure 2-3 also shows where the **Help** button is now located on the Navigation bar of the new Administrative Console.

Common Administrative Console Features

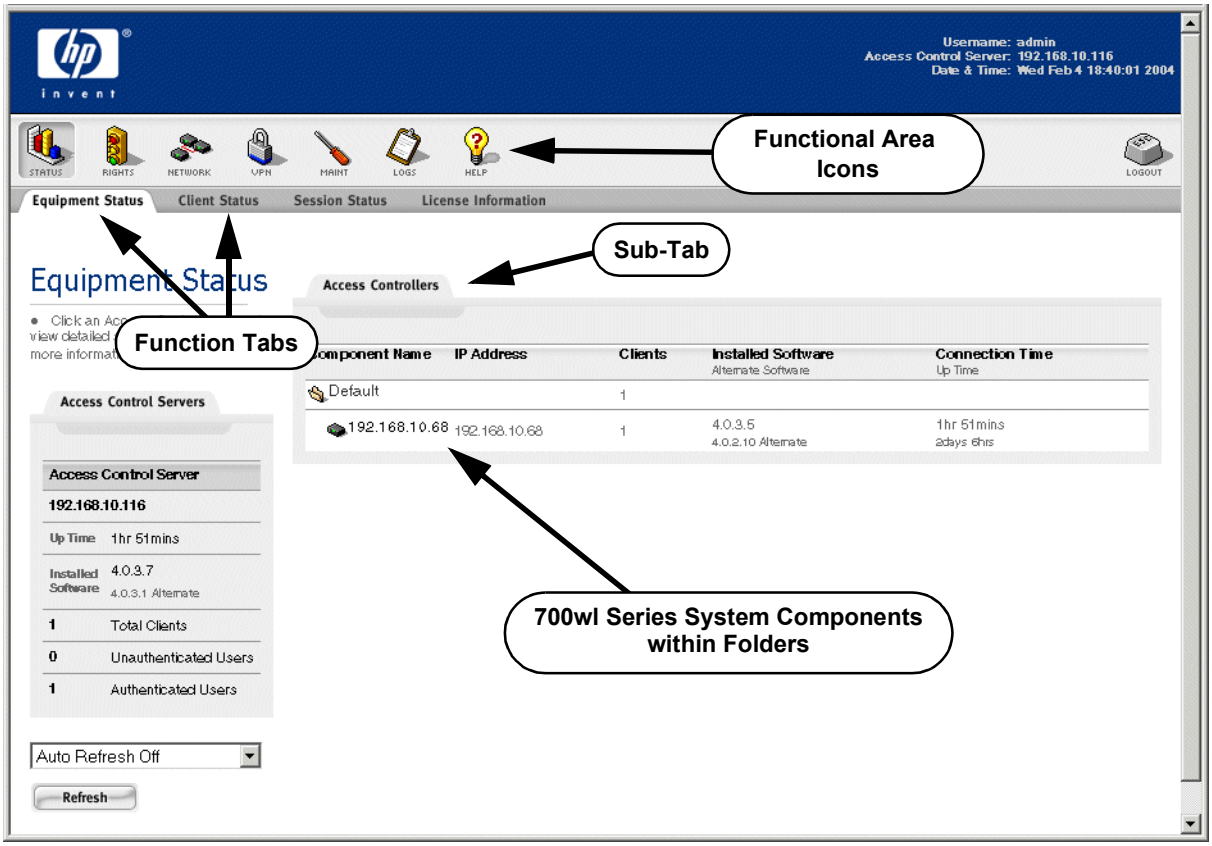
The new Administrative Console uses a set of common visual features consistently throughout the entire interface. This section explains the meaning and use of these.

Common Page Layout Features

Figure 2-4 shows some of the common page layout features of the new Administrative Console:

- Functional areas are organized into sections. Each section has its own tab at the top of every page for that functional area. These *function tabs* appear just under the Navigation bar. You move between sections of the functional area by clicking the appropriate tab. The currently active tab is shown in white. Tabs for other sections of the current functional area are greyed out. In Figure 2-4 the **Equipment Status** tab is the currently active tab, the others (**Client Status** and **Session Status**) are greyed out.
- Functional areas with a lot of configuration options have *sub-tabs*. These sub-tabs appear near the top of the page (see the sub-tab in Figure 2-4 and the sub-tabs in Figure 2-5). These work the same as tabs.

Figure 2-4. Common Page Layout Features



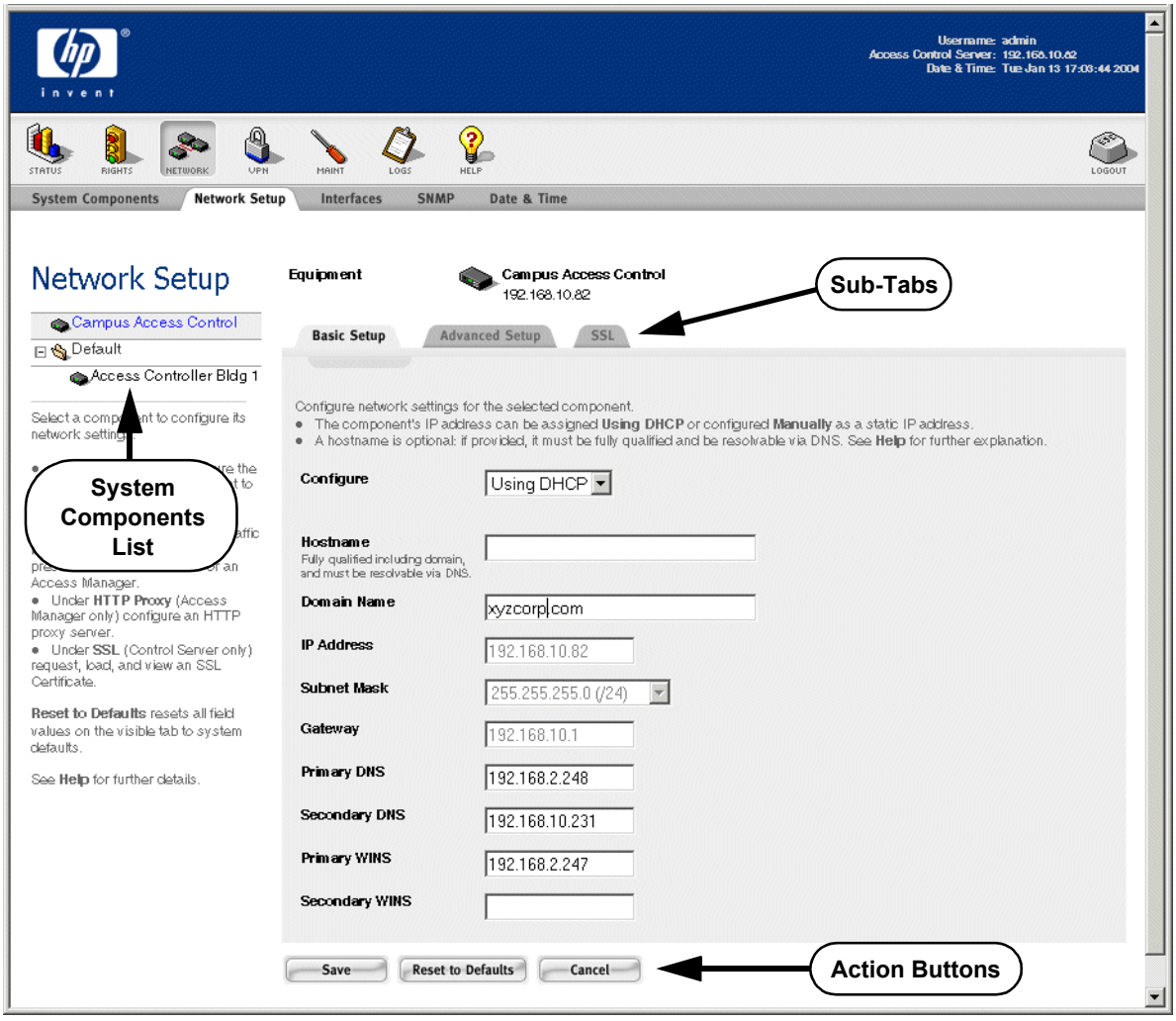
- On pages where you configure and manage the 700wl Series system components, those components are organized in a structured list that you create to match the organization of your network. You do this by creating folders and assigning equipment to a folder.

  Folders are indicated by a folder icon ( ) as shown in Figure 2-4. Folders can be opened to show their contents or they can be closed to allow you to simplify or abbreviate the display.

Figure 2-5 shows additional common features of the Administrative Console:

- On pages where you need to apply commands to specific HP ProCurve equipment, a concise version of the system components list appears on the left of the page. The folders in this list can be opened and closed to display the equipment. To configure or maintain a specific component, click on the component in the System Components List to select it. The selected component is highlighted and the page changes to display the current settings for that component. Any changes you make are applied to the selected component.

Figure 2-5. More Common Page Layout Features



- Most pages contain buttons for performing system configuration actions (see *Action Buttons* in Figure 2-5). For example, many pages have buttons at the bottom of the page for saving the current settings, canceling any changes you may have started to make, or restoring the settings on the page to the default settings.

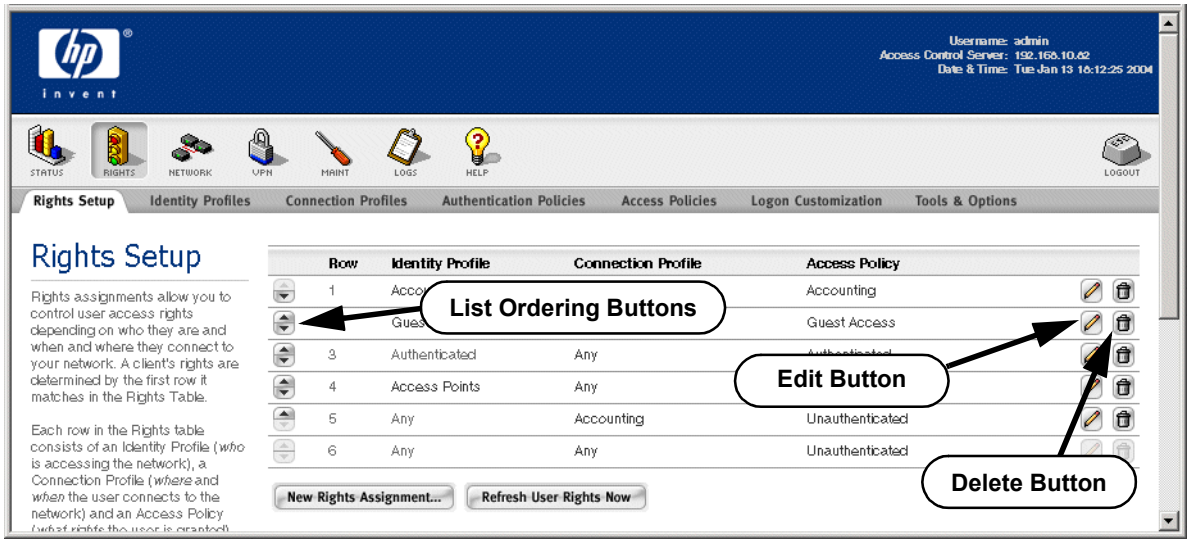
  Three trailing dots (**...**) following the button label indicate that the button brings up a new page for performing the specified function, depending on the button label. Figure 2-6 on page 2-7 shows an example of this (the **New Rights Assignment...** button).

  Note: *In most cases when you click an action button on a page that has sub-tabs, the action applies to the contents of all the sub-tabs. For example, in Figure 2-5 clicking the* ***Save*** *button saves any changes that were made on the current sub-tab (****Basic Setup****) as well as any changes that were made on the other sub-tabs (****Advanced Setup*** *and* ***SSL****).*

Table and List Manipulation

Figure 2-6 shows common icons used for manipulating the items in a table or list.

Figure 2-6. Common Table Manipulation Icons (part 1)



- Some items are managed by use of an ordered list. In the new Administrative Console you explicitly order these lists by using the list ordering button to the left of the item in the list ( ).

  The list ordering button normally has two active parts. Click the up arrow to move the item up one position in the list; click the down arrow to move the item down one position in the list. If the item cannot be moved in a particular direction the arrow for that direction is grayed out.

  Some built-in items have a fixed position in the list, such items have their list ordering button completely grayed out. For instance the Rights table has an "Any Identity/Any Connection/Unauthenticated Access" combination that is the "fall-through" or default match for clients that do not match any other profile; this is always at the bottom of the list.

- To operate on items in a table or list, used the buttons on the right side of the row the item is in. Figure 2-5 shows the common buttons for editing an item ( ) and for deleting an item ( ).

Figure 2-7. Common Table Manipulation Icons (part 2)

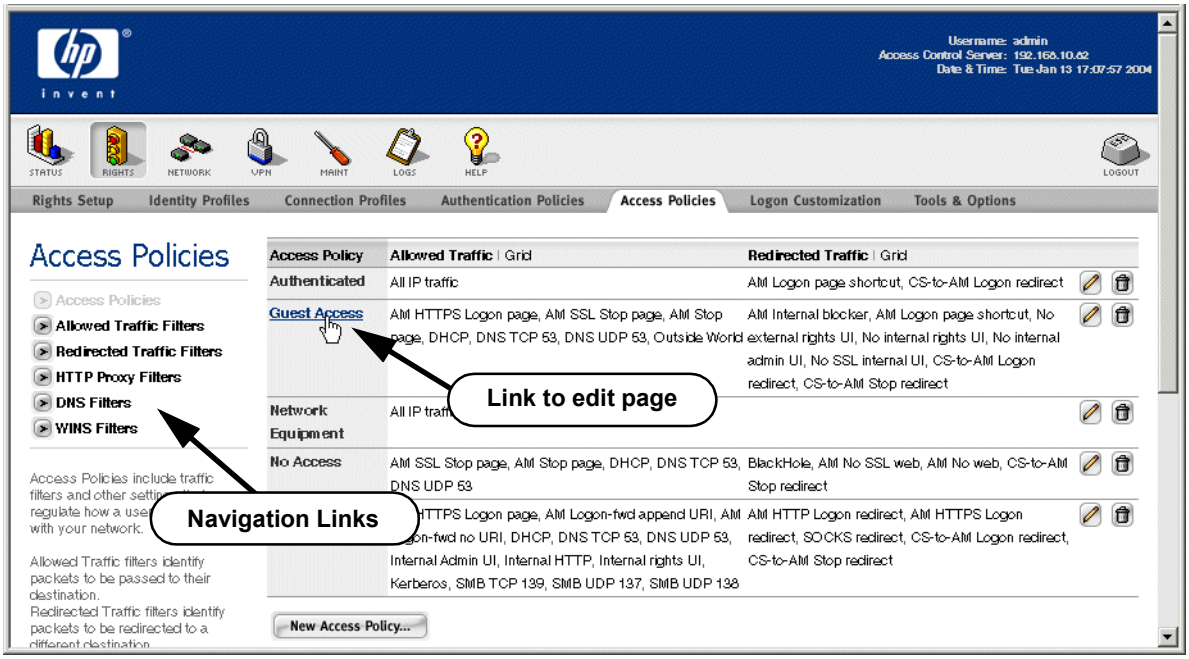


Figure 2-7 shows additional features of the new Administrative Console:

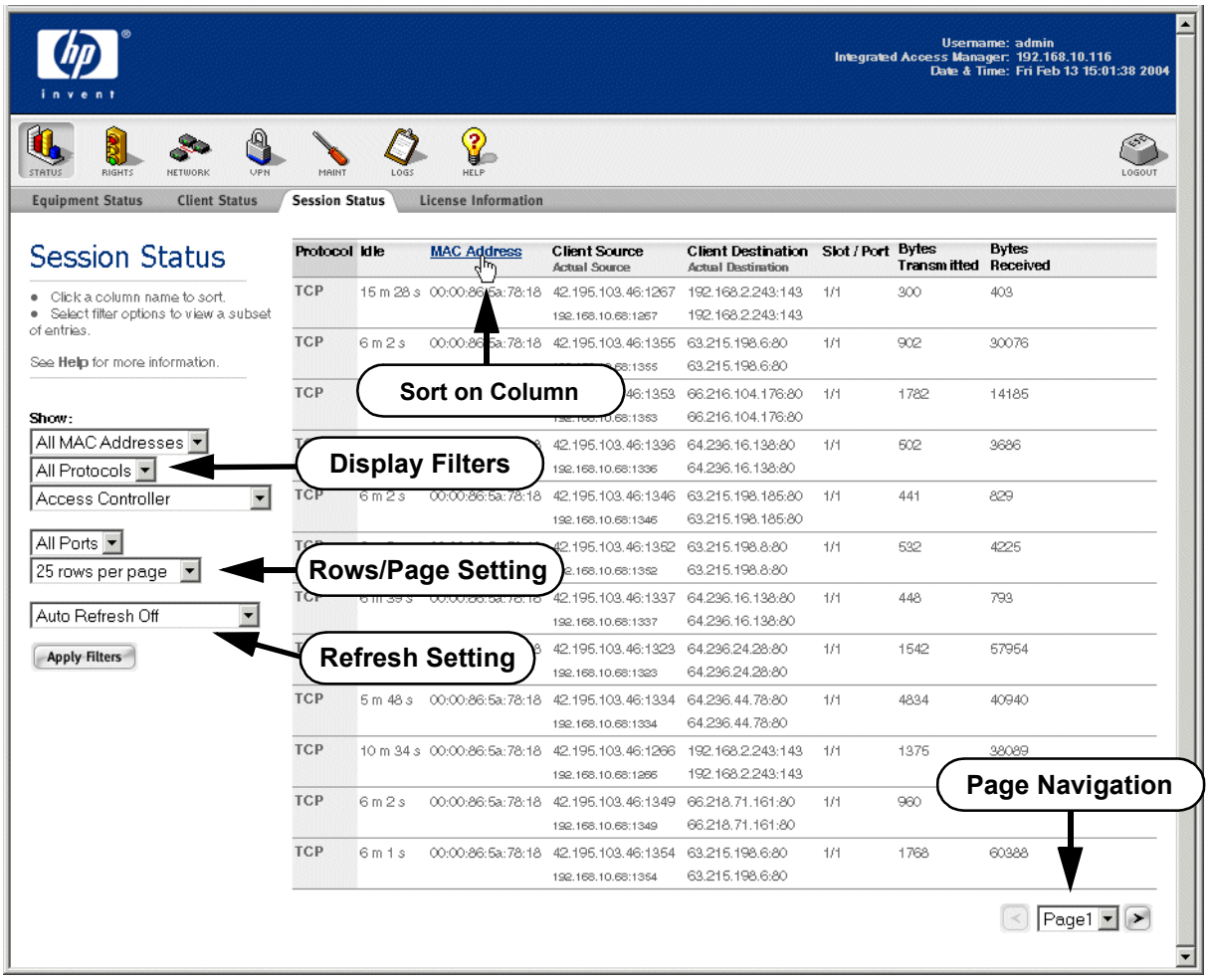
- In tables you edit an item in the table by clicking on that item. Row items that are links to the page for editing that item change color and are underlined when the cursor moves over the item name. The cursor also changes to show that the item is a link (for instance the mouse cursor changed to a pointing finger when it moved over **Guest Access** in the list of Access Policies in Figure 2-7).
- On some pages you can toggle among different related functions or views of the system data. This is indicated by a set of links on the left of the page immediately under the page's title. These navigation links are indicated by an arrow button ( ). Clicking on the link to the right of this button takes you to that page. The current page is grayed out in the list of related pages, see *Navigation Links* in Figure 2-7.

  For example, in Figure 2-7 the current page is for configuring **Access Policies** (the **Access Policies** link is grayed out). From this page, by clicking the appropriate navigation links, you can go directly to various other pages to view and configure filters that may be used within an Access Policy.

Active Display Features

In the Status and Logs functions, on pages that display dynamic data, you can set the page to automatically refresh the data after a specified interval. To do this you select the desired refresh interval (or select **Auto Refresh Off**) and click the **Apply Filters** or **Refresh** button. The button is labelled **Apply Filters** on pages where the dynamic information can be filtered. See *Refresh Setting* in Figure 2-8 and the **Refresh** button in Figure 2-4.

Figure 2-8. Active Display Features



- If a table contains more than 25 rows, the table is displayed in multiple pages with 25 rows per page. 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 ( ) to go directly to a specific page.

  You adjust the number of rows per page to display by selecting the number of rows to display on a page in the rows/page setting pulldown, see *Rows/Page Setting* in Figure 2-8. This setting is applied when you click **Apply Filters**. Any auto-refresh setting you select is also applied when you click **Apply Filters**.
- Another way to control the display of information is provided by display filters. These are located on the left side of the page, see *Display Filters* in Figure 2-8. To filter the displayed information, select the desired filter values and click **Apply Filters**. This refreshes the display with data that matches the filter criteria.
- 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 (change color and show as underlined) when the cursor moves over the

column name (as shown in Figure 2-8). In some tables, such as the Log Files or Session Status display, where there are multiple items shown in a column, you may be able to sort on each item in the column separately (this is the case with the example in Figure 2-8).

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 2-8 the display is ordered based on the **Protocol** column.

Common Buttons and Icons

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

Table 2-1. Administrative Console Buttons/Icons

Icon	Meaning
	Folder: This represents a user-defined folder for system components. Folders can be opened, revealing their contents, by clicking on the open folder icon (⊞). They can be closed by clicking on the close folder icon (⊟). See Figure 2-5 for an example of this icon. This icon is used in the System Components List.
	Access Control Server, Integrated Access Manager or Access Controller: This represents a system component. These icons are used in the System Components List, and also on pages in the Network and Maintenance areas along with other identifying information (name or IP address) to identify the component that is being configured.
	Secondary Access Control Server in a redundant configuration. This icon is used in the System Components List
	Edit button: Click this button to edit the object in the same row. For example, to edit a Connection Profile in the Connection Profiles table.
	Delete: Click this button to delete the object in the same row. For example, to delete an Access Controller from the System Components table.
	List Ordering Button: These buttons appear in a list, such as Rights Assignment table, where the order of items in a list is significant. Click the top half of this button to move the current row up in the list; click on the bottom half to move it down in the list.
	View: Click this button to view related information, for example, to view the login page associated with a Connection Profile on the Edit Connection Profile page. See Figure 2-23 for an example of this button.
	Configure: Click this button to configure the object in the same row. For example clicking this button for an authentication service in the MAC Address Retrieval table brings up the Configure MAC Address Retrieval page for that authentication service. See Figure 2-23 for an example of this button.
	Download: Click this button to download data from the source in the same row. For example clicking this button for an authentication service in the MAC Address Retrieval table downloads the MAC Address data from that authentication service. See Figure 2-23 for an example of this button.
	Refresh Rights: Click this button to update the rights for the client in the same row. This applies the currently specified rights, and is normally done after the rights have been changed. See Figure 2-30 for an example of this button.
	Logout: Click this button to logout the client in the same row. See Figure 2-30 for an example of this button.

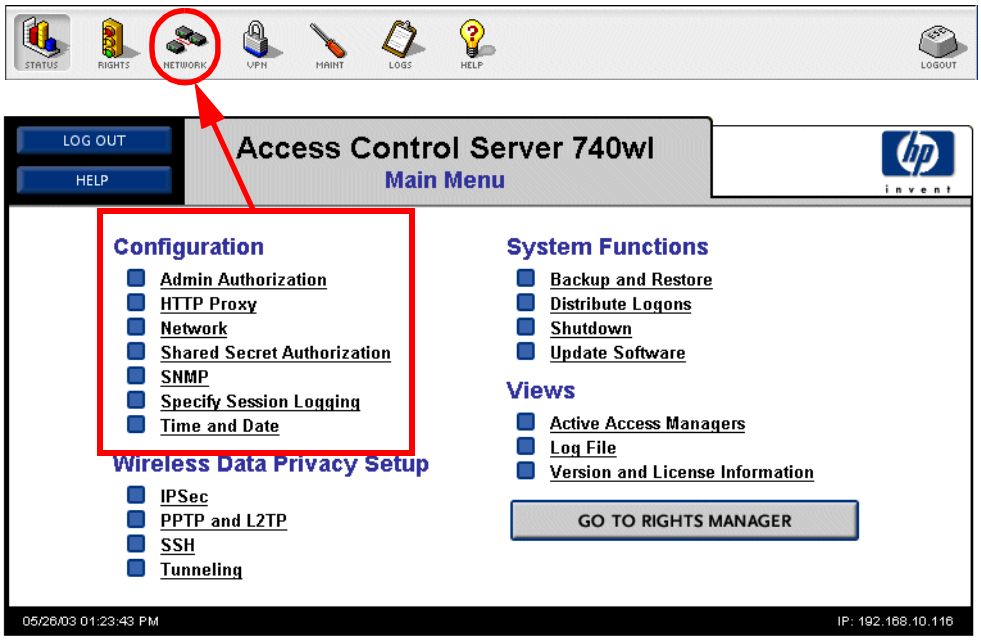
Main Menu Configuration Links (the Network Area)

The functional areas of the 700wl Series system have been reorganized in the new Administrative Console to improve the workflow. This and the following sections of this chapter show where to find the system tasks and functions in the new Administrative Console. With the exception of the Rights Manager, the information on most pages under the new Administrative Console is similar to the information that was on the corresponding page of the old Administrative Console.

This and the sections that follow are organized based on the 3.1 software user interface to help you find familiar tasks and functions.

Most of the functions that were under the **Configuration** link in the version 3.1 Administrative Console Main Menu are now found in the **Network** area of the new Administrative Console, accessed by clicking the **NETWORK** button on the Navigation bar of the new Administrative Console.

Figure 2-9. Where to find the Configuration functions



What's Changed

- With the new Administrative Console you configure all the 700wl Series system equipment from one Administrative Console on the Access Control Server. You no longer have to go to the Administrative Console for each Access Controller; all the configuration and maintenance tasks can be done through the Administrative Console for the Access Control Server.

  When system components are added to the 700wl Series system the primary Access Control Server will recognize them and automatically perform the initial configuration. All that needs to be set on an Access Controller before it is connected to the network is the IP address of the Access Control Server and the Access Control Server's shared secret, so that the Access Control Server can recognize it as a trusted Access Controller.

- You can now configure redundant peer Access Control Servers to ensure high availability. A redundant peer Access Control Server takes over administration of the 700wl Series system automatically if the primary Access Control Server can no longer function.
- The functions found on the old Admin Authorization page, including changing the administrator logon name and password and enabling technical support access, are now configured with the other configuration information, under the System Components tab of the Network module.
- The specification of session logging has been expanded and moved to the logs area. To specify session logging go to the **Logging Setup** tab of the Logs areas. See "Logging Setup" on page 2-36.
- **Specify Location Information** is now incorporated into the configuration of an Access Controller, and is handled under the new Rights Manager when setting up Connection Profiles.
- Specifying an HTTP Proxy server for an Access Controller is now part of the configuration of the Access Controller.
- The port configuration functions found on the Advanced Network Configuration page in the 3.1 Administrative Console are now found under the Interfaces tab in the Network area.

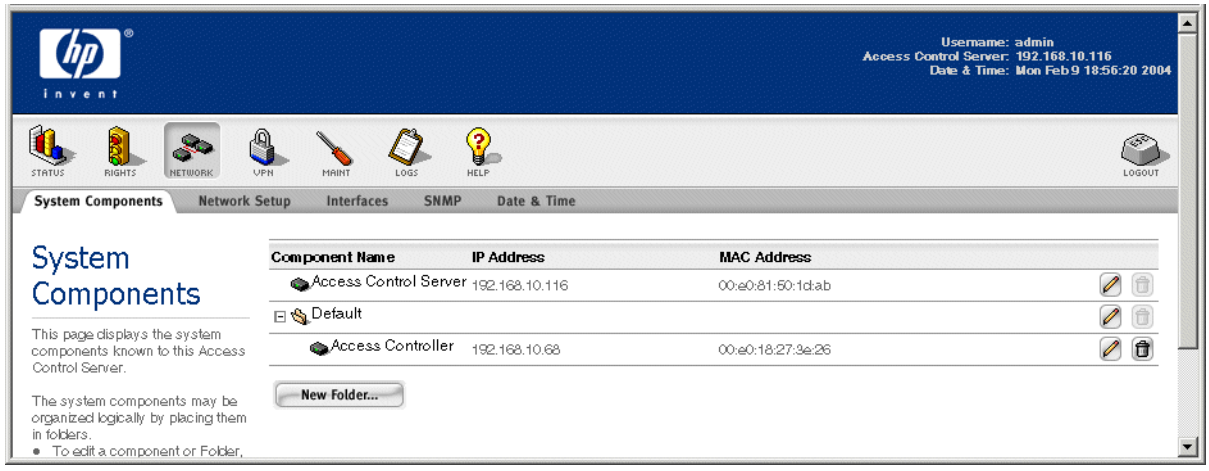
The System Components Tab

The system components area is where you specify the identity of your 700wl Series system components. The system components may be organized logically by placing them in folders.

» Click the **System Components** tab in the Network area, as shown in Figure 2-10.

This brings up the System Components page.

Figure 2-10. The Network Area: System Components



» To edit a component or Folder, click its name or the pencil icon at the right.

» To delete an component or Folder, click the trash can button. A Folder must be empty to be deleted.

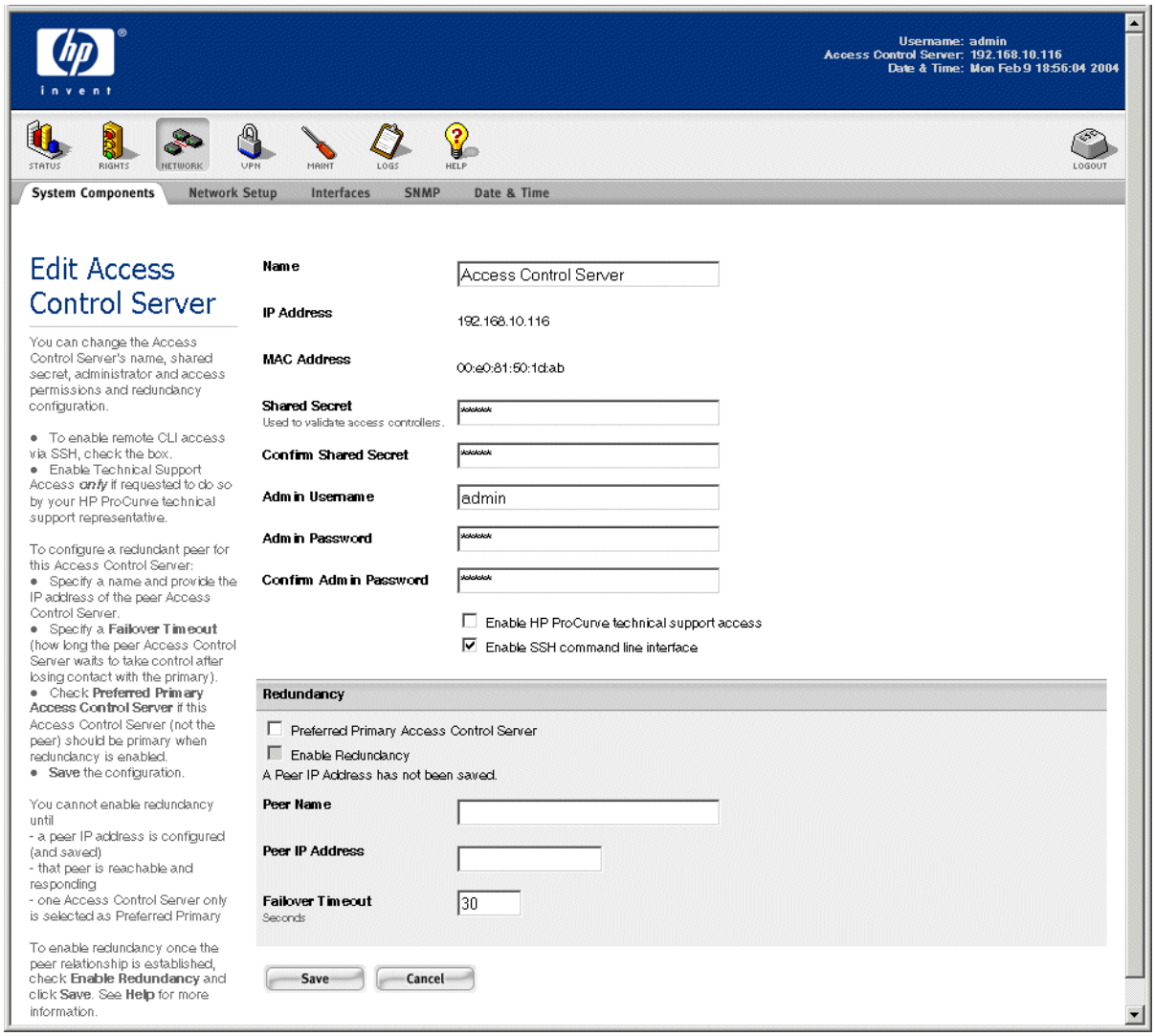
Editing the Access Control Server

If you select an Access Control Server to edit, the Edit Access Control Server page appears. See Figure 2-11. On this page you can:

- Give a name to the Access Control Server
- Change the currently used shared secret. This change will be propagated automatically to all the currently active Access Controllers.
- Change the Administrator Username and Password
- Enable technical support access to the Access Control Server (if appropriate)
- Enable an SSH command line interface to the Access Control Server (a new feature)
- Configure a peer Access Control Server to act as a redundant Access Control Server, and specify whether this Access Control Server should be considered the primary Access Control Server if there is contention between the two peers.

See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for details of the new features.

Figure 2-11. The Network Area: Edit Access Control Server



Access Controller

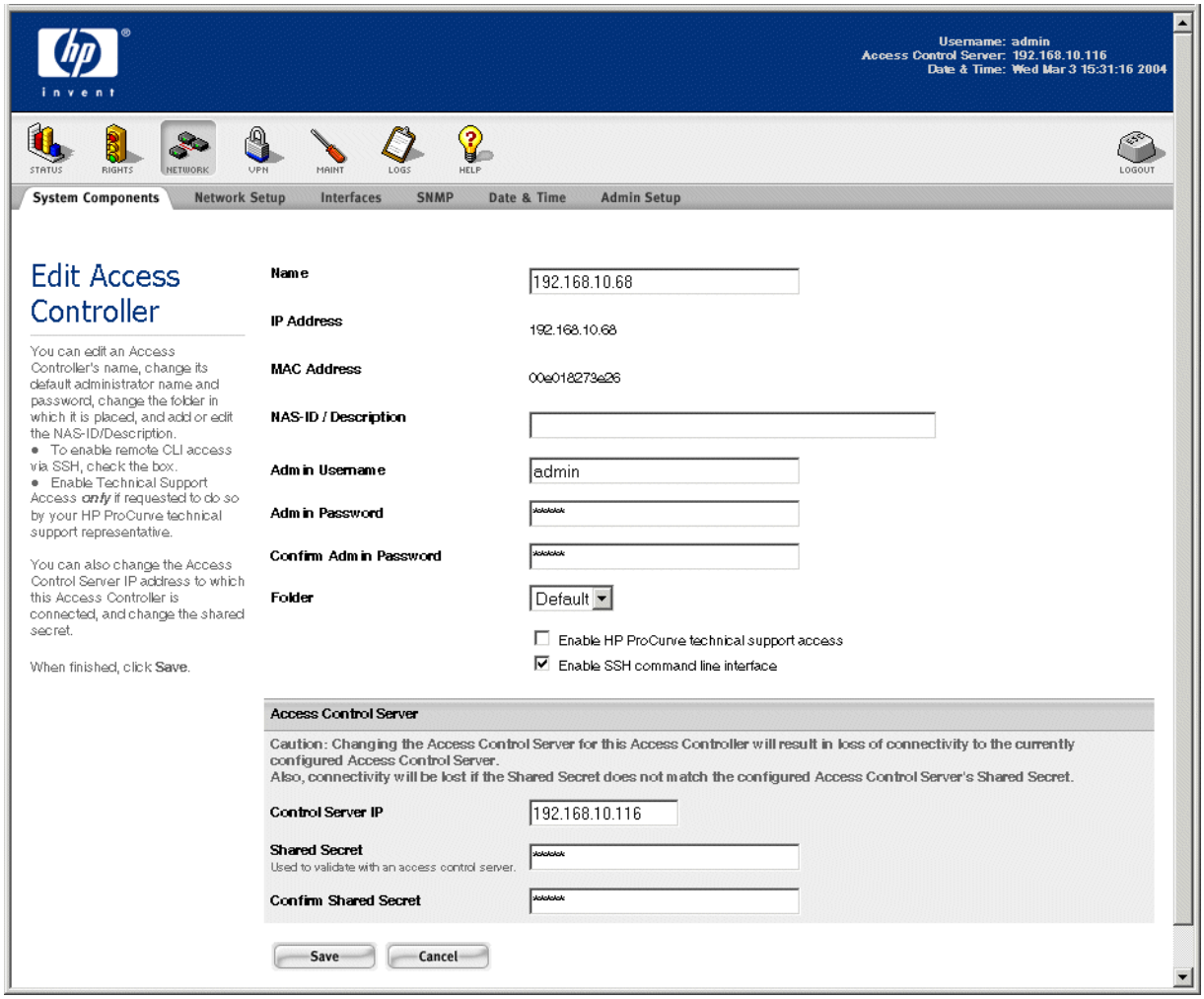
An Access Controller appears in the System Components List as soon as it is installed on the network and configured with the correct Access Control Server IP address and shared secret.

If you select an Access Controller to edit, the Edit Access Controller page appears. See Figure 2-12. On this page you can:

- Give a name to the Access Controller
- Provide an optional description or NAS-ID (for use with RADIUS accounting)
- Place the Access Controller into a folder
- Enable technical support access to the Access Controller (if appropriate)
- Enable an SSH command line interface to the Access Controller (a new feature)

- Change the Access Control Server IP address and shared secret, to disconnect the Access Controller from its current Access Control Server and connect it to a different Access Control Server

Figure 2-12. The Network Area: Edit Access Controller



The Network Setup Tab

The Network Setup area is where you specify the network settings for your 700wl Series system components. These vary depending on whether you are configuring an Access Control Server or an Access Controller.

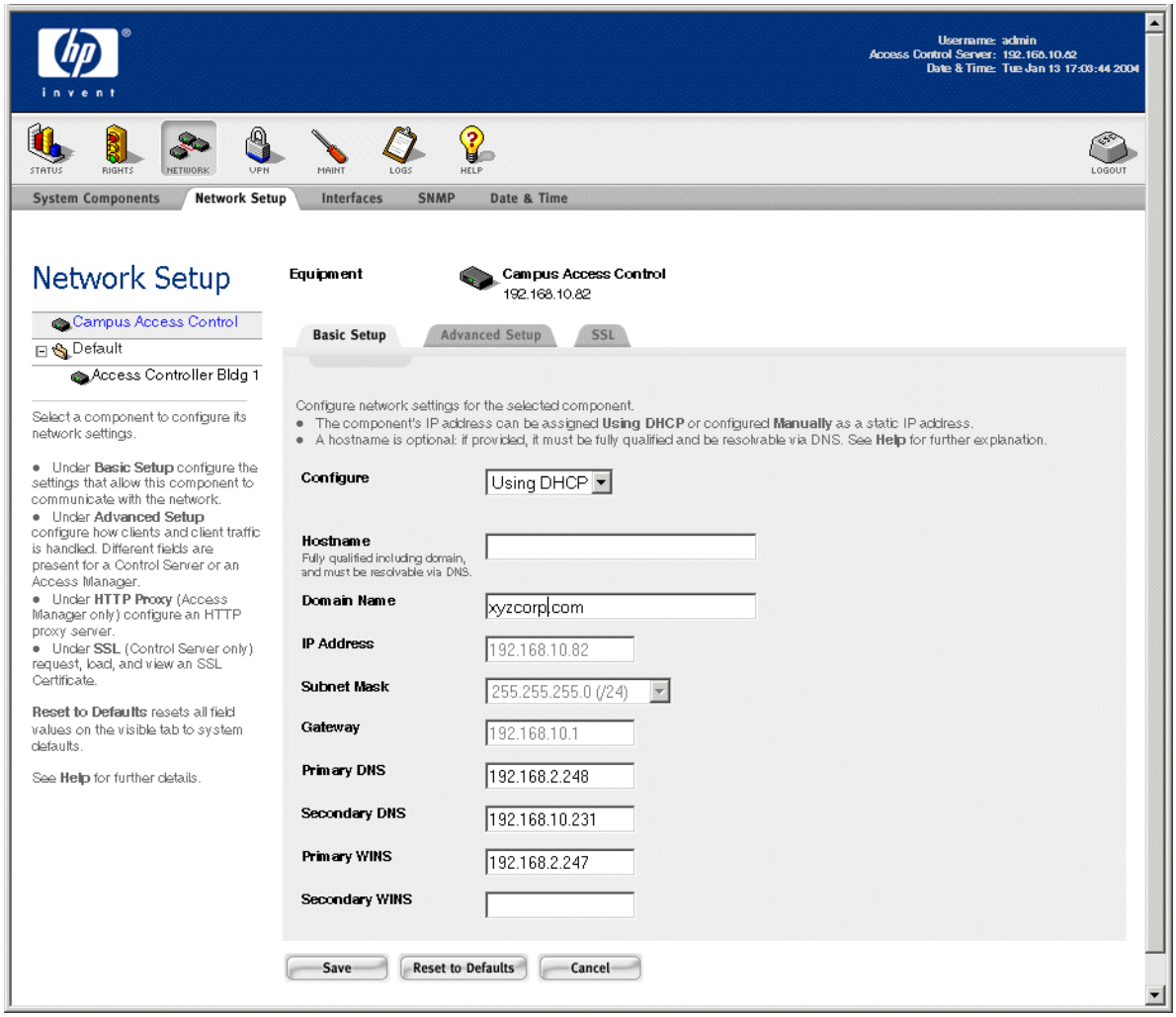
» Click the **System Components** tab in the **Network** area, see Figure 2-13.

This displays the Network Setup page. Initially, this displays the setting for the Access Control Server on which you are running the Administrative Console. For an Access Control Server there are three sub-tabs:

- **Basic Setup**—This is where you specify how the IP address is assigned, the hostname (optional), the subnet mask, the gateway, and the primary and secondary DNS and WINS.

- **Advanced Setup**—This is where you configure the internal DHCP server settings used to provide addresses for NAT'ed clients.
- **SSL**—This is where you generate CSR requests and load SSL certificates and private keys.

Figure 2-13. The Network Area: Network Setup for an Access Control Server



Access Controller

» To configure the network settings for an Access Controller, click on the Access Controller from the system component list in the left panel of any Network Setup page.

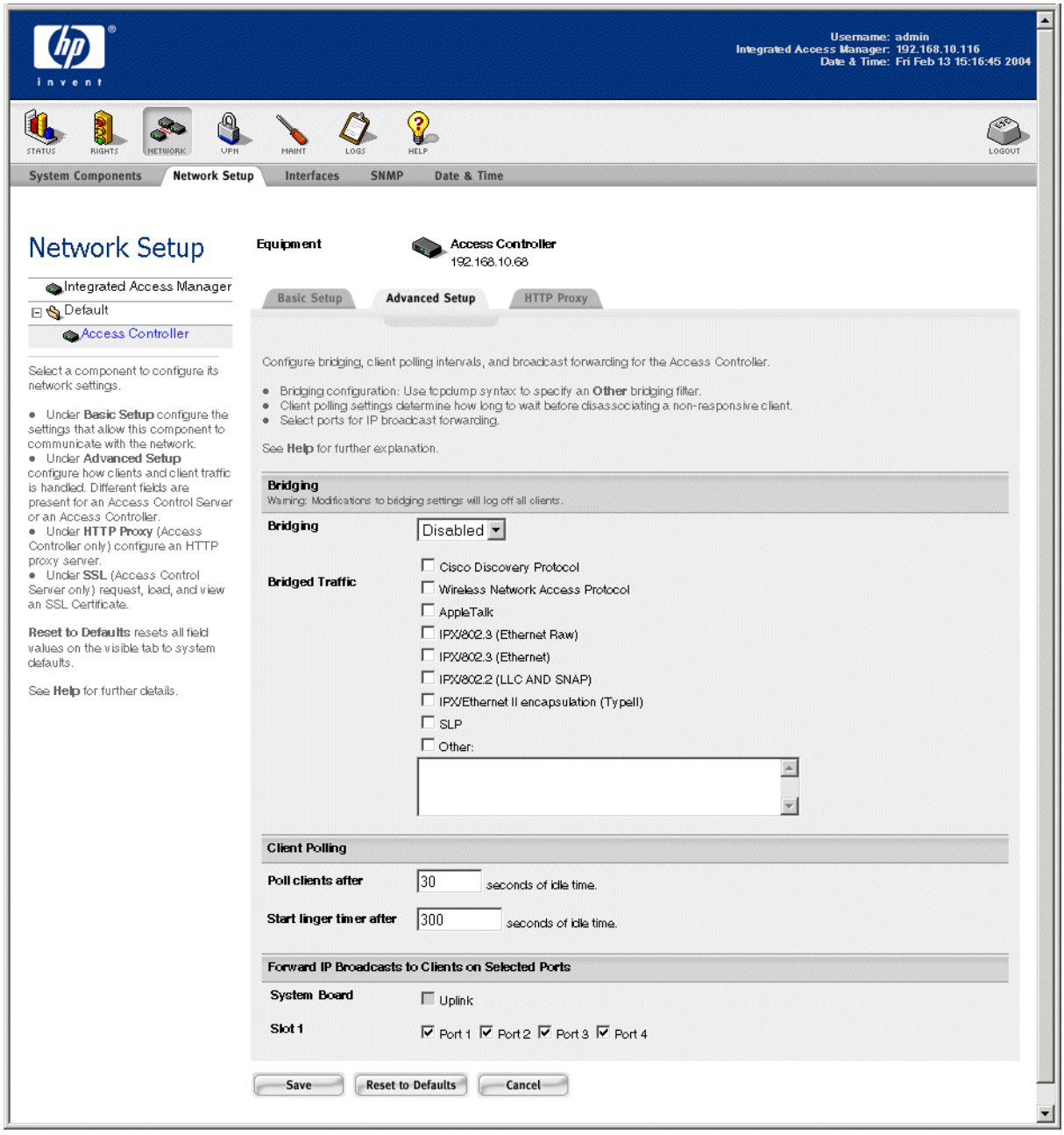
The Network Setup page for that Access Controller appears. The initial sub-tab is similar to that for an Access Control Server.

For an Access Controller there are three sub-tabs:

- **Basic Setup**—This is where you specify how the IP address is assigned, the hostname (optional), the subnet mask, the gateway, and the primary and secondary DNS and WINS.

- **Advanced Setup**—This is where you configure the bridging configuration, client polling (how long to wait for non-responsive clients), and whether to forward IP broadcasts to clients on specified ports. See Figure 2-14.
- **HTTP Proxy**—This is where you specify the server IP address and port for any HTTP proxy used by this Access Controller.

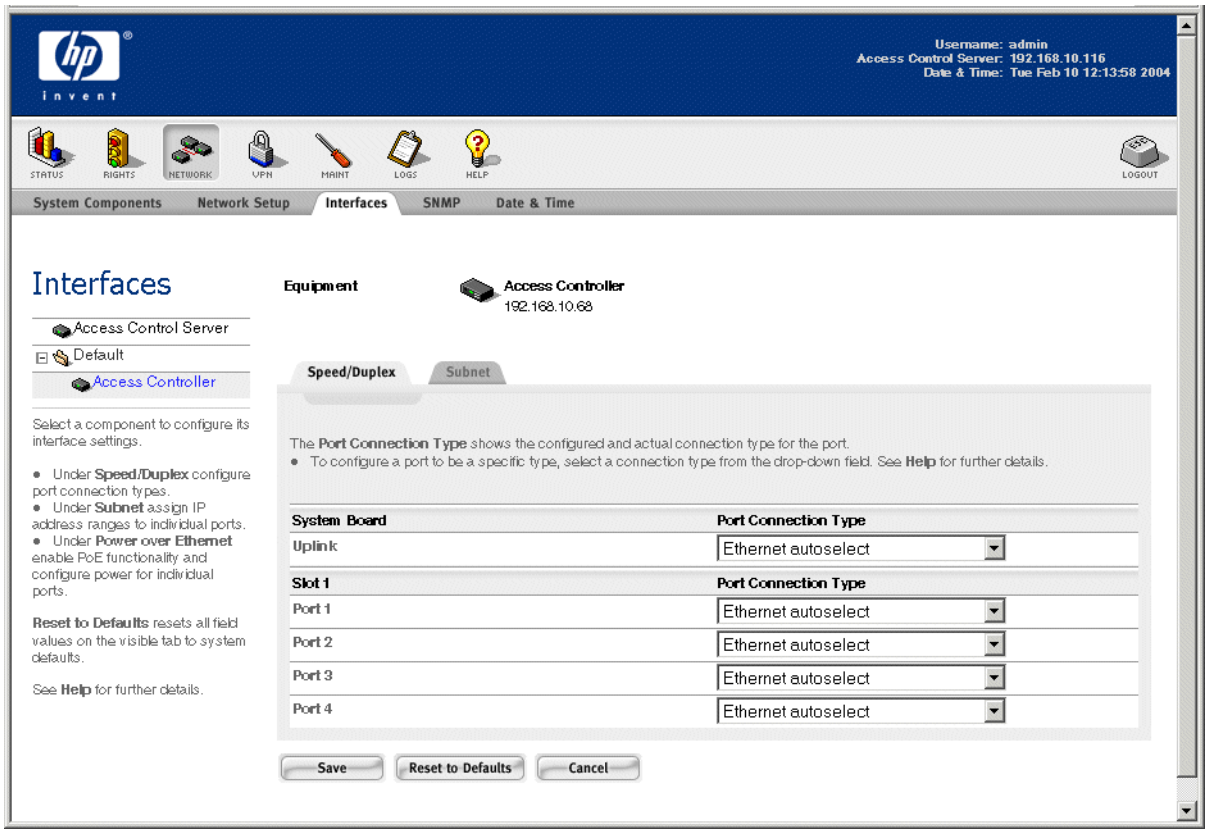
Figure 2-14. The Network Area: Network Setup for an Access Controller



The Interfaces Tab

Port settings for Access Controllers and Integrated Access Managers are no longer part of the advanced setup page. Port settings are now located under the **Interfaces** tab under the Network area. To view and configure port settings, click **NETWORK**, then the **Interfaces** tab. The Interfaces page appears, as in Figure 2-15.

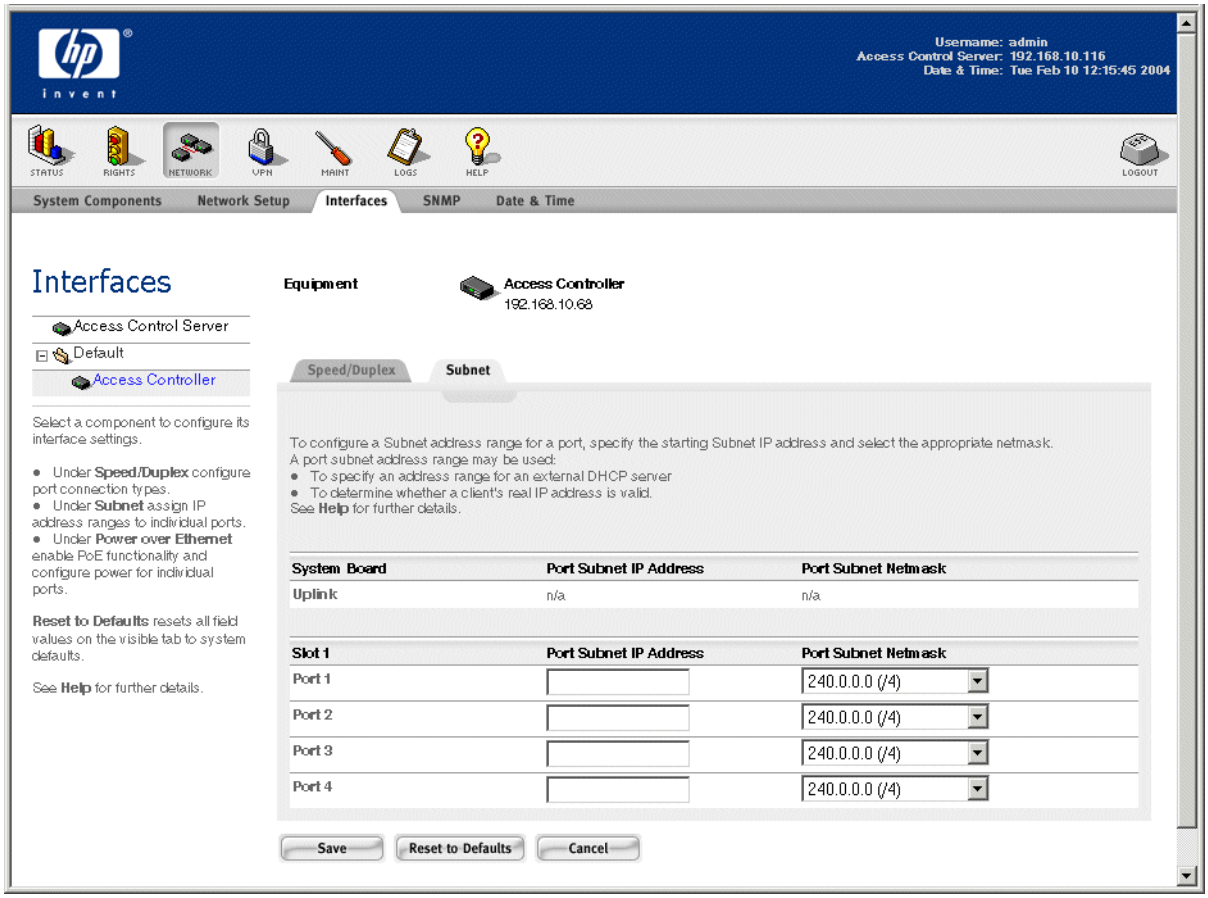
Figure 2-15. The Network Area: Interfaces: Speed/Duplex Tab



Click the appropriate component from the System Components List in the left panel. The page displays again with the interface information for that component. The port settings are divided across two sub-tabs.

- The **Speed/Duplex** tab is where you set the connection speed and duplex setting for each port.
- The **Subnet** tab is where you set the Port Subnet IP Address and Port Subnet Netmask for each port. See Figure 2-16.

Figure 2-16. The Network area: Interfaces: Subnet Tab



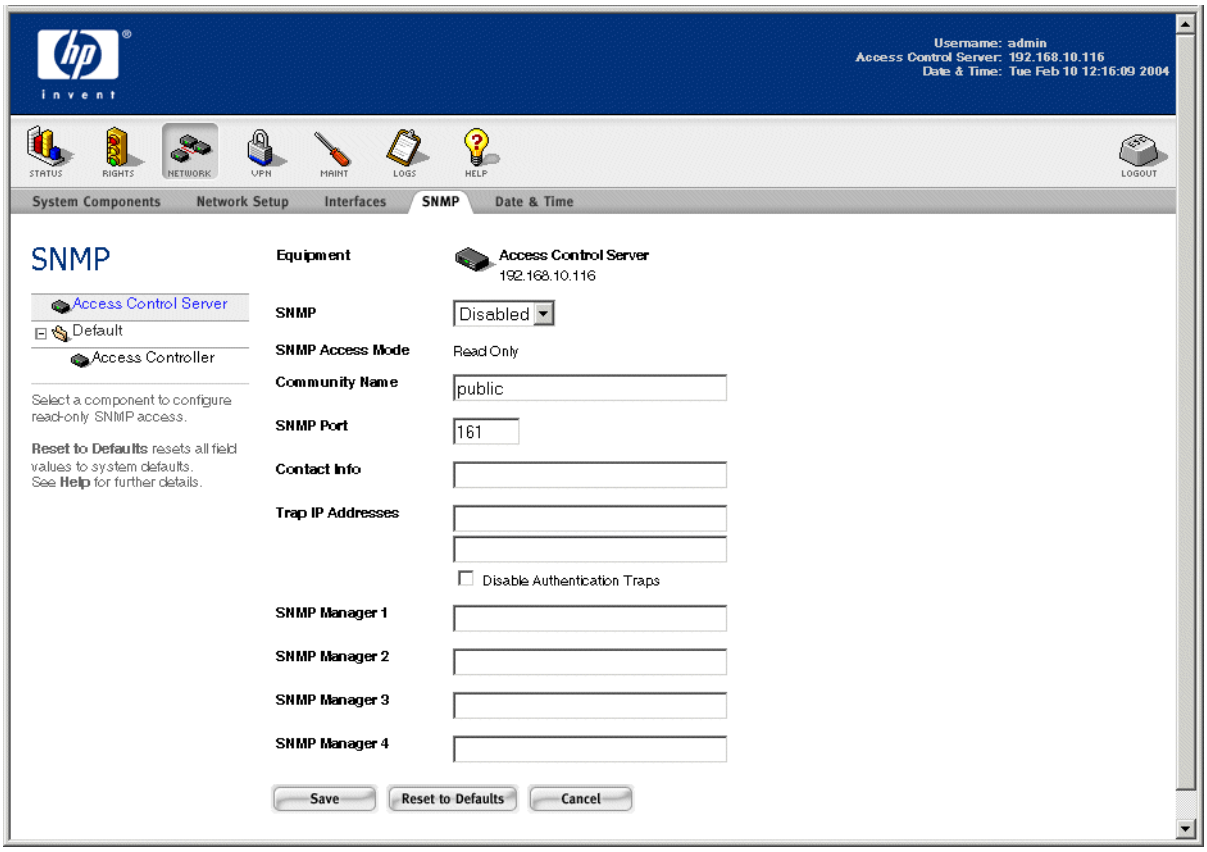
The settings on these two pages are very similar to the port settings under the Advanced Network Configuration page in the old (3.1) user interface.

The SNMP Tab

To configure the SNMP settings so that the 700wl Series system can be monitored by a network management system, click the **SNMP** tab in the Network area. The SNMP page appears, see Figure 2-17.

The settings on this page are basically the same as on the SNMP page in the 3.1 Administrative Console. Enter the appropriate information and click **Save**.

Figure 2-17. The Network Area: SNMP



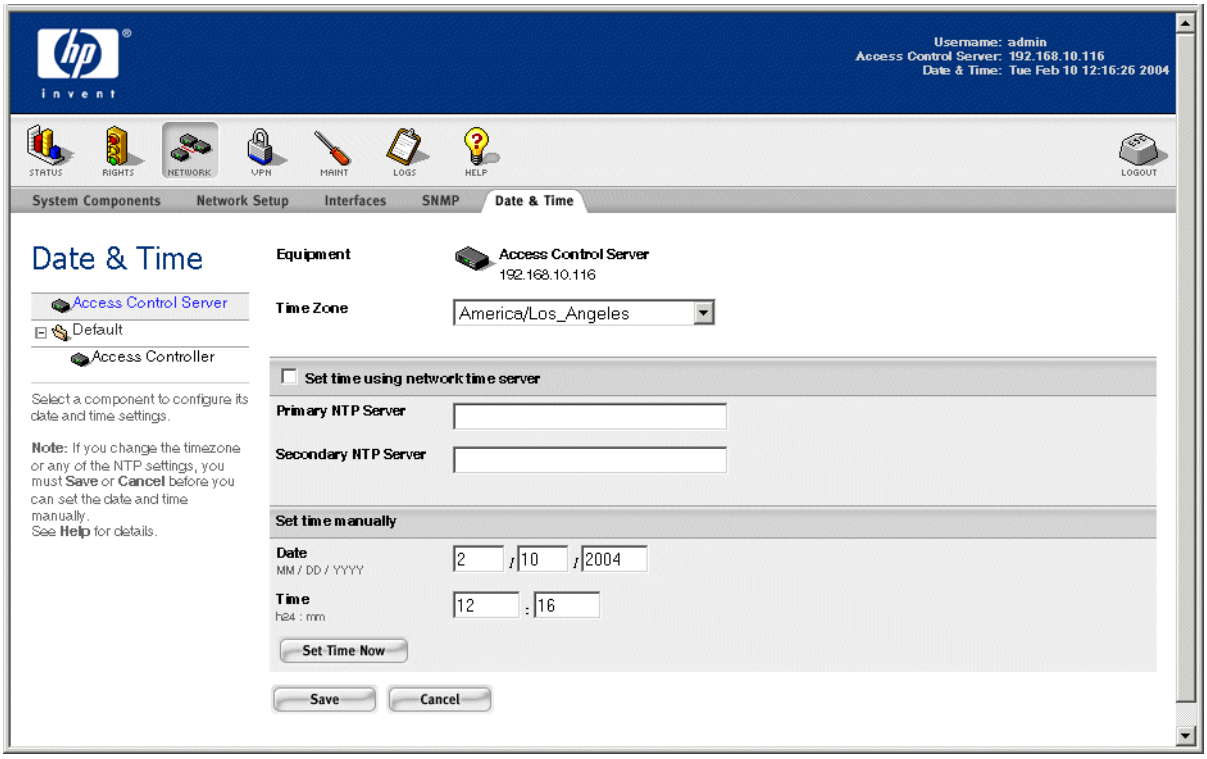
The Date and Time Tab

To set the time, time zone, and date for a 700wl Series system component, click the **Date & Time** tab under **NETWORK** (see Figure 2-18). In the System Components List in the left panel select the component for which you wish to set the date and time. The page displays again with the current date and time information for that component.

On the **Date & Time** tab you can:

- Set the component's time zone
- Specify whether you want the time to be set and maintained by a Network Time Protocol (NTP) server, and specify the IP address for the primary and secondary NTP server.
- Manually specify the date and time. Note that you can set the date and time manually and also configure an NTP server to maintain the time. (Setting the time manually can be useful when making large time adjustments.)

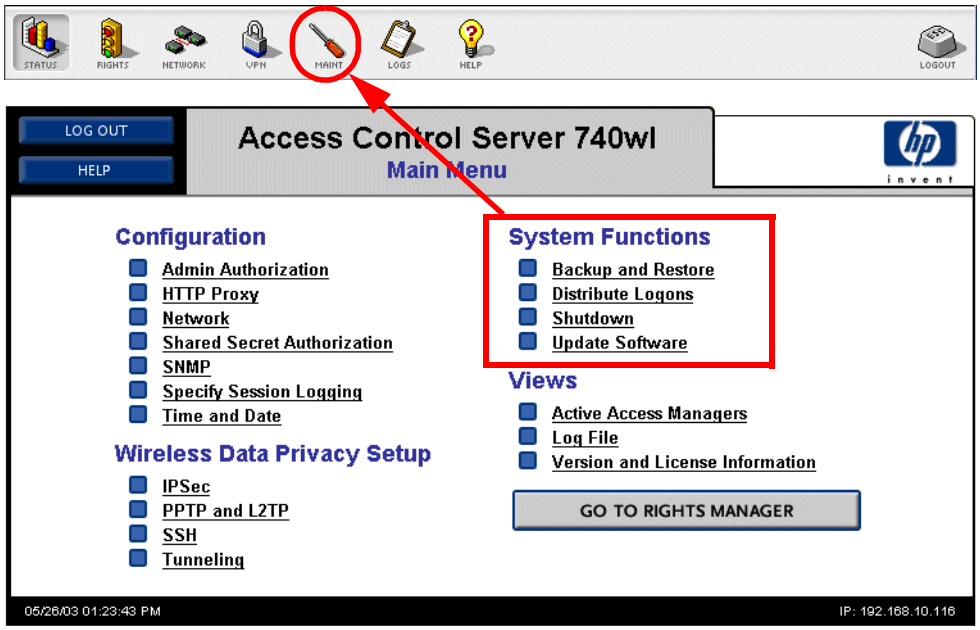
Figure 2-18. The Network Area: Date & Time



Main Menu System Functions (the Maintenance Area)

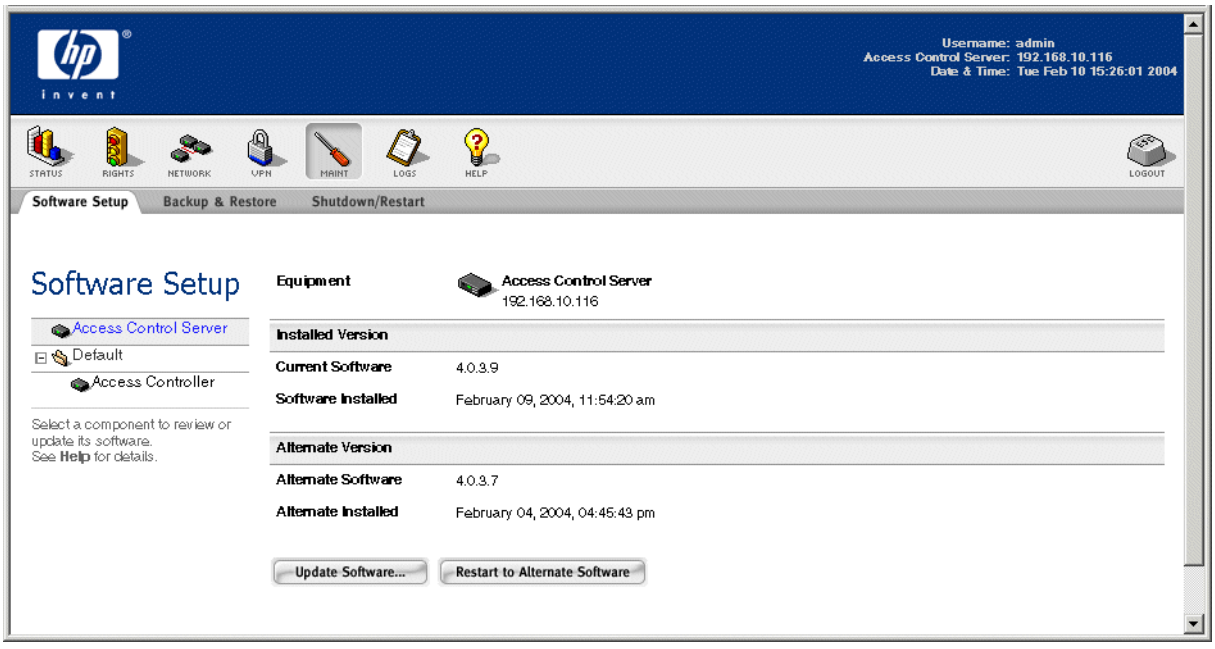
The actions that were under **System Functions** on the Main Menu of the 700wl Series system 3.1 Administrative Console are now found under the Maintenance area (the **MAINT** button), as shown in Figure 2-19.

Figure 2-19. Where to Find the System Function Pages



Click **MAINT** to go to the Maintenance area. Figure 2-20 shows the Software Setup tab, which is the initial page that is displayed in the Maintenance area.

Figure 2-20. The Maintenance Area: Software Setup Tab



In the Maintenance area you can do the following:

- Update the system software for 700wl Series system

- Backup and restore the 700wl Series system settings, logs, and rights (the 700wl Series system database). This backs up the configuration of the Access Control Server (or Integrated Access Manager) and all connected Access Controllers.
- Shutdown and restart 700wl Series system components.

What's Changed

- With the new Administrative Console you can perform these system functions on all Access Controllers and a peer Access Control Server from a single centralized interface on the Access Control Server or Integrated Access Manager. To manage a specific component, select the component from the System Components List in the left panel. The right panel changes to reflect the current settings for that component. Any changes you make and save apply to that component.
- It is no longer necessary to back up or restore your Access Controllers individually. Since Access Controller configuration is done and stored centrally, Access Controller configuration data is backed up along with the Access Control Server configuration information. If you reset an Access Controller to factory defaults, once it reconnects to the Access Control Server (after configuring the Access Control Server IP address and shared secret) the Access Controller configuration will be propagated to the Access Controller by the Access Control Server.
- The **Distribute Logons** option is no longer necessary. Logon processing is always distributed, i.e., logons are handled by the Access Controllers, not the Access Control Server. This greatly enhances logon performance.
- "Update Software" is now labelled "Software Setup"
- "Shutdown" is now "Shutdown/Restart"

The Software Setup Tab

To update the 700wl Series system software on any 700wl Series system component managed by this Access Control Server, click the **Software Setup** tab under the Maintenance area (see Figure 2-20.) In the System Components List in the left panel select the component for which you wish to update or check the installed software. The page displays again with the Software Setup information for that component.

The **Software Setup** tab summarizes the installed and alternate software versions for the selected component. From this tab you can:

- Reboot to the alternate version of the system software.
- Update the system software.

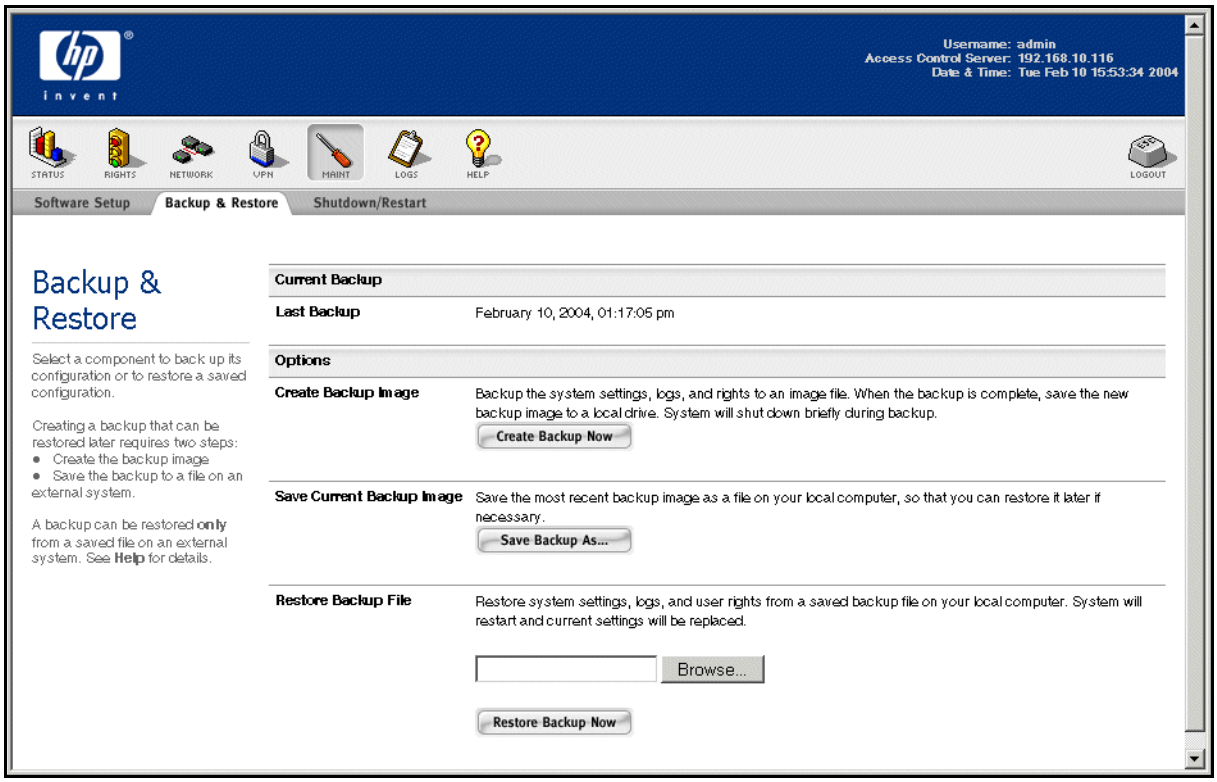
  The update process is the same as with 700wl Series system 3.1.

Each Access Control Server and Access Controller can maintain two versions of the system software. You can reboot the system either to upgrade the system software or return it to the previous version of the software.

The Backup and Restore Tab

To backup or restore the 700wl Series system settings, logs, and rights data, click the **Backup & Restore** tab under the maintenance area. See Figure 2-21.

Figure 2-21. The Maintenance Area: Backup & Restore Tab



Backing up the 700wl Series system database works the same as with version 3.1—first, you create the backup image, then you save the image to a file on your system's hard disk. However, unlike version 3.1, the configuration for the Access Control Server or Integrated Access Manager and all connected Access Controllers is backed up in one operation.

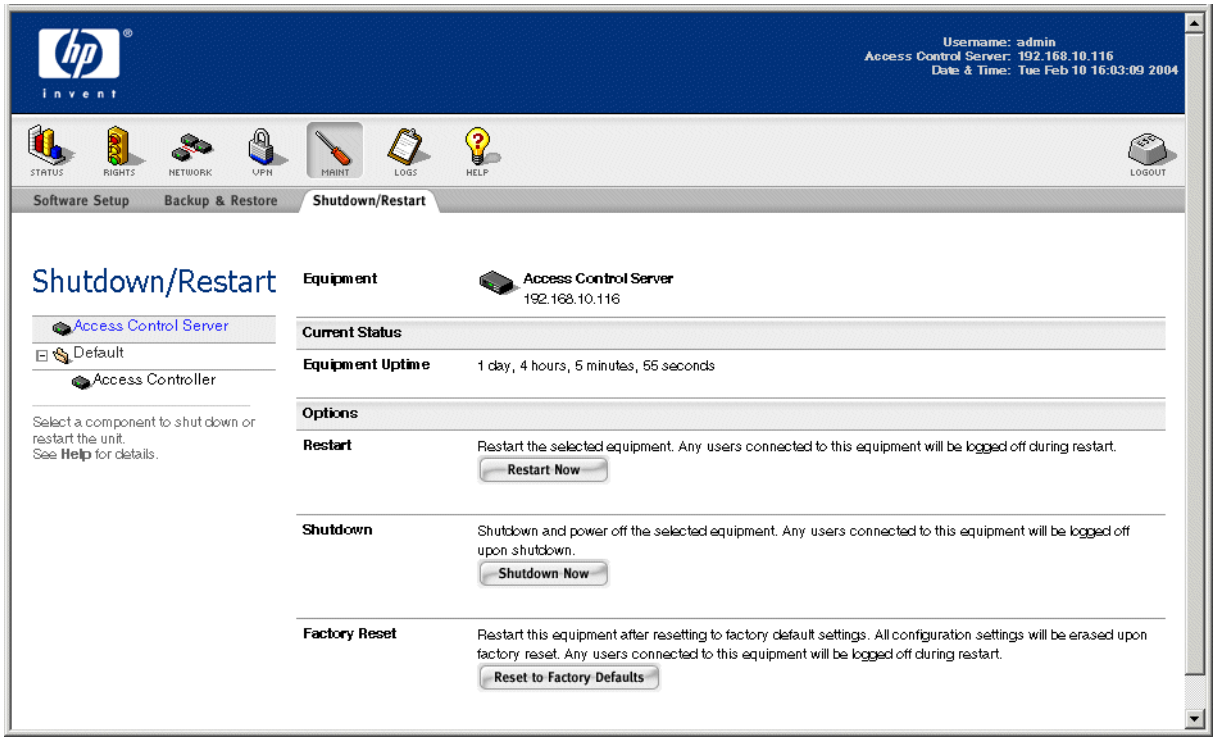
To backup or restore your 700wl Series system, click the **Backup & Restore** tab. The backup is always made from the database on the Access Control Server that you are currently logged into as Administrator.

- Click **Create Backup Now** to create a backup of the system settings, logs, and rights. This is stored internally on your Access Control Server or Integrated Access Manager.
- Click **Save Backup As …** on the Backup and Restore page to download the backup image to a local directory.
- To restore a previously saved system backup, click the **Browse** button under **Restore Backup File** to find and select the saved backup file, then click **Restore Backup Now**.

The Shutdown/Restart Tab

To shutdown or restart any 700wl Series system component, click the **Shutdown/Restart** tab under the Maintenance area (see Figure 2-22).

Figure 2-22. The Maintenance Area: Shutdown/Restart Tab



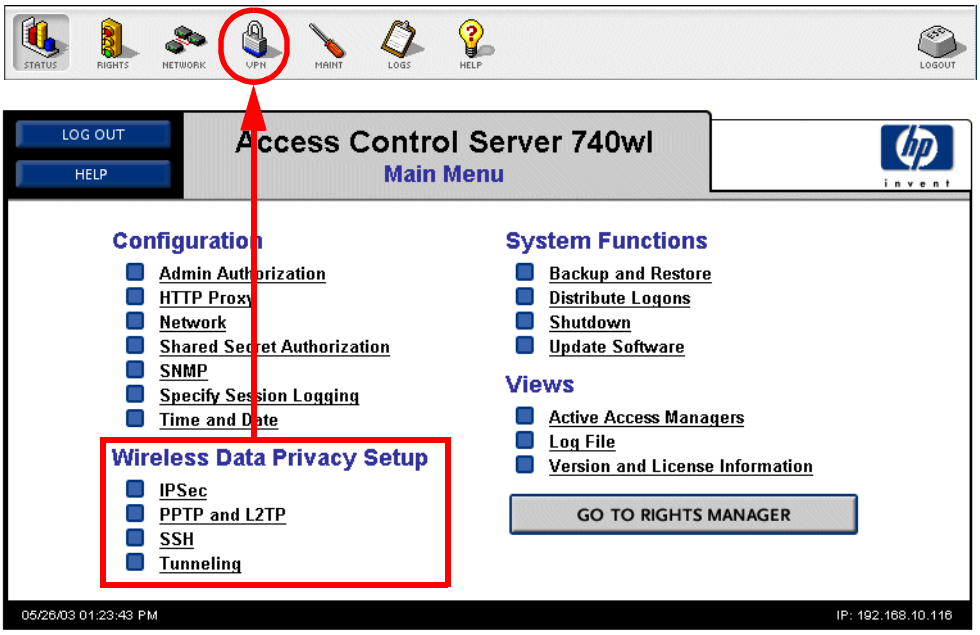
Select the target component from the System Components List in the left panel. The page displays again with the Shutdown/Restart information for that component.

As with version 3.1, you can choose to reboot the unit (**Restart Now**), shut down a unit (**Shutdown Now**) or reset the unit to its Factory Defaults (**Reset Now**).

Main Menu Wireless Data Privacy (the VPN Area)

The functions that were under Wireless Data Privacy Setup in the old Administrative Console have been placed in the VPN area. See Figure 2-23.

Figure 2-23. Where to find the Wireless Data Privacy Setup pages



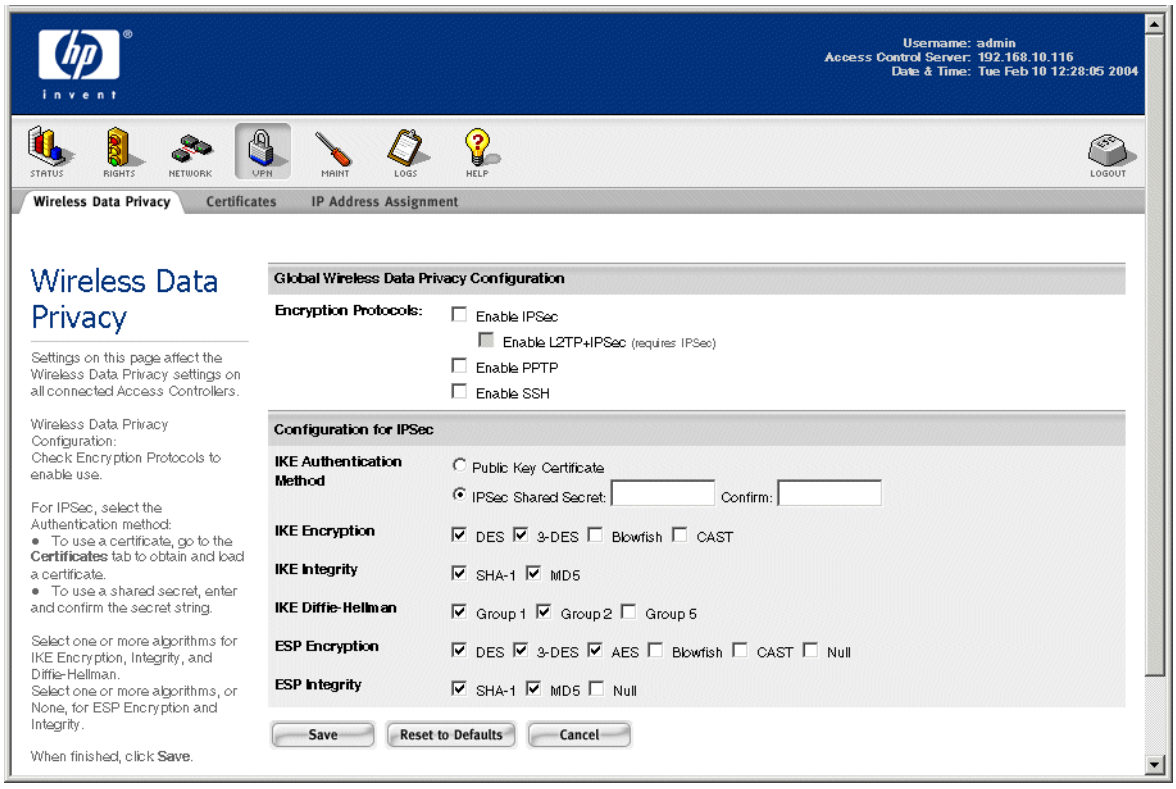
What's Changed

- The **IPSec**, **PPTP and L2TP**, and **SSH** configuration pages have been combined into a single page, the Wireless Data Privacy tab under the VPN area.
- In version 4.0, IPSec is enabled automatically when you enable L2TP.
- The Certificate installation process for IPSec has its own tab under the VPN area.

The Wireless Data Privacy Tab

When you click **VPN**, the Wireless Data Privacy tab is displayed. Under the Wireless Data Privacy tab, you can globally enable or disable the security protocols—L2TP plus IPSec, IPSec alone, PPTP, and/or SSH. Figure 2-24 shows the Wireless Data Privacy tab.

Figure 2-24. VPN: the Wireless Data Privacy Setup Tab



The configuration settings for IPSec (IKE and ESP authentication and encryption) are the same as in version 3.1. See the *700wl Series System Management and Configuration Guide* for a detailed explanation.

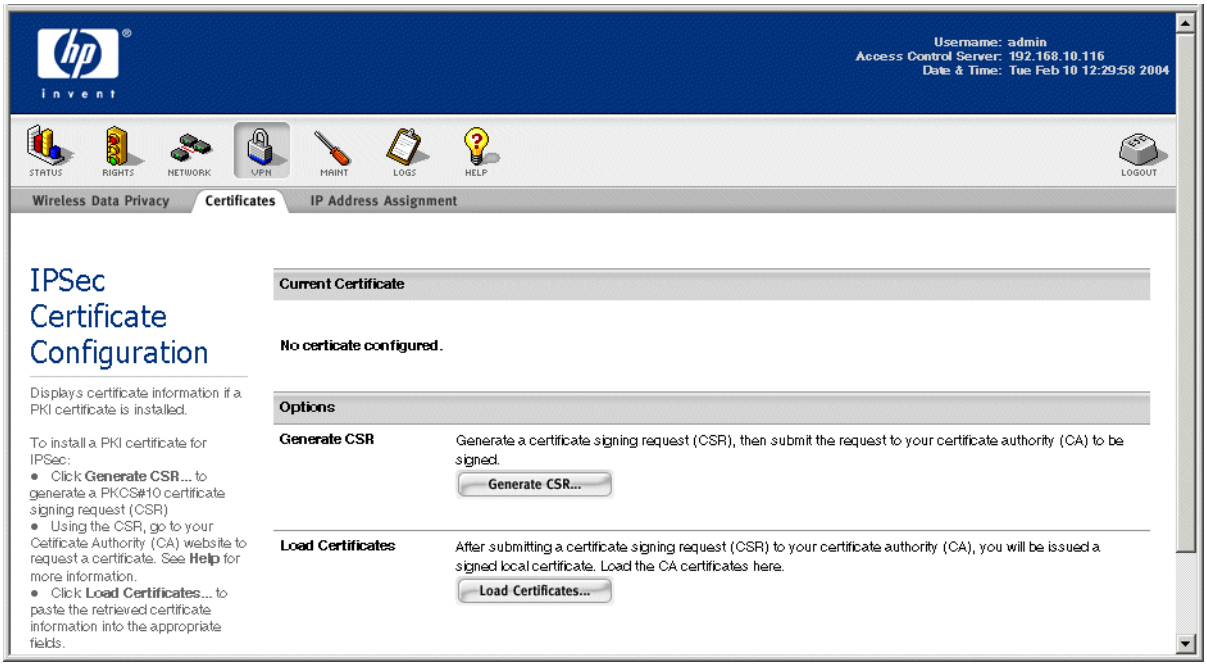
Once you have enabled the appropriate security protocols, you can specify whether those protocols are allowed or required as part of an Access Policy. In version 3.1 these settings were configured per Location. See Chapter 3, "The New Rights Manager" for more details on setting up Access Policies.

If you want to use a public key certificate for IPSec, you generate the certificate signing request (CSR) on the **Certificates** tab of the VPN area. When you receive the certificate from the certificate authority you load it into the system on this same page.

The Certificates Tab

The Certificates tab (shown in Figure 2-25) lets you generate a Certificate Signing Request, and load the resulting certificates into the 700wl Series system. This page is very similar to the IPSec Certificate Configuration page accessed using the **Configure Certificate** button from the IPSec Configuration page in the 3.1 Administrative Console.

Figure 2-25. VPN: The Certificates Tab

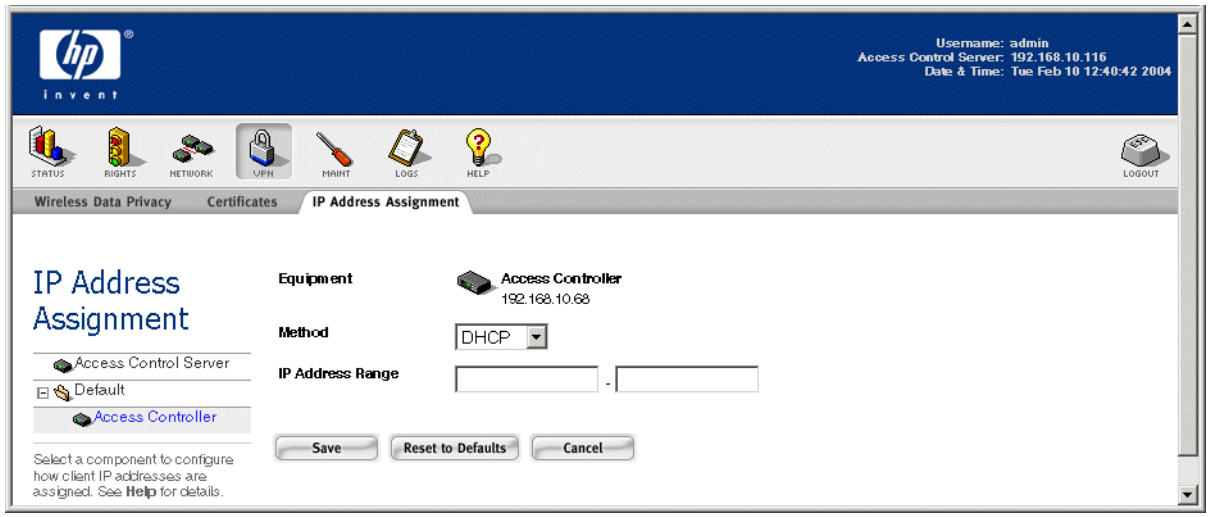


See the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* for more details on configuring certificates for IPSec.

The IP Address Assignment Tab (Tunneling)

If you plan to use IPSec or PPTP/L2TP for Wireless Data Privacy, you must configure the method by which your Access Controller assigns the inner tunnel address used by a client using one of the tunneled security protocols. As with version 3.1, a different tunneling method can be configured per Access Controller. Figure 2-26 shows the IP Address Assignment page—it is basically the same as the Tunneling configuration page in version 3.1.

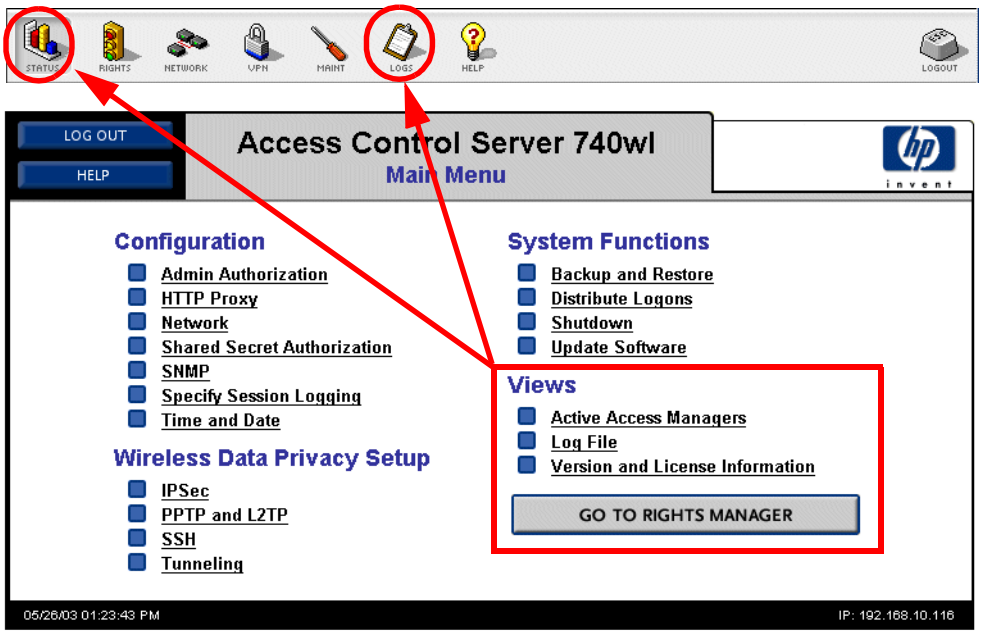
Figure 2-26. VPN: IP Address Assignment



Main Menu Views (the Status and Logs Areas)

The functions that were under "Views" in 700wl Series system 3.1 are now split between the Status area and the Logs area. Figure 2-27 shows where the **STATUS** and **LOGS** buttons are located on the Navigation bar of the new Administrative Console. Click **STATUS** to go to the Status area (see Figure 2-28). This is also the initial page you see when you logon to the Administrative Console of the 700wl Series system. Click **LOGS** to go to the Logs area (see Figure 2-33).

Figure 2-27. Where to find the Views pages



What's Changed

All the functionality available under the **View** heading in 700wl Series system 3.1 is still available. Changes have been made to make system monitoring easier:

- With the new Administrative Console you can view the status and logs for all the 700wl Series system equipment from one Administrative Console located on the primary Access Control Server. You no longer have to go to the Administrative Console for each Access Controller.
- All status information is accessible from the Status area. This includes both the **Views** section of the old **Main Menu** and client status information that was previously found under the Rights Manager.
- The Status views have been redesigned and enhanced to make them more readable and easier to manage.
- All the log information, including the information found in the Rights Manager log in version 3.1, has been combined and is accessible from the Logs area.

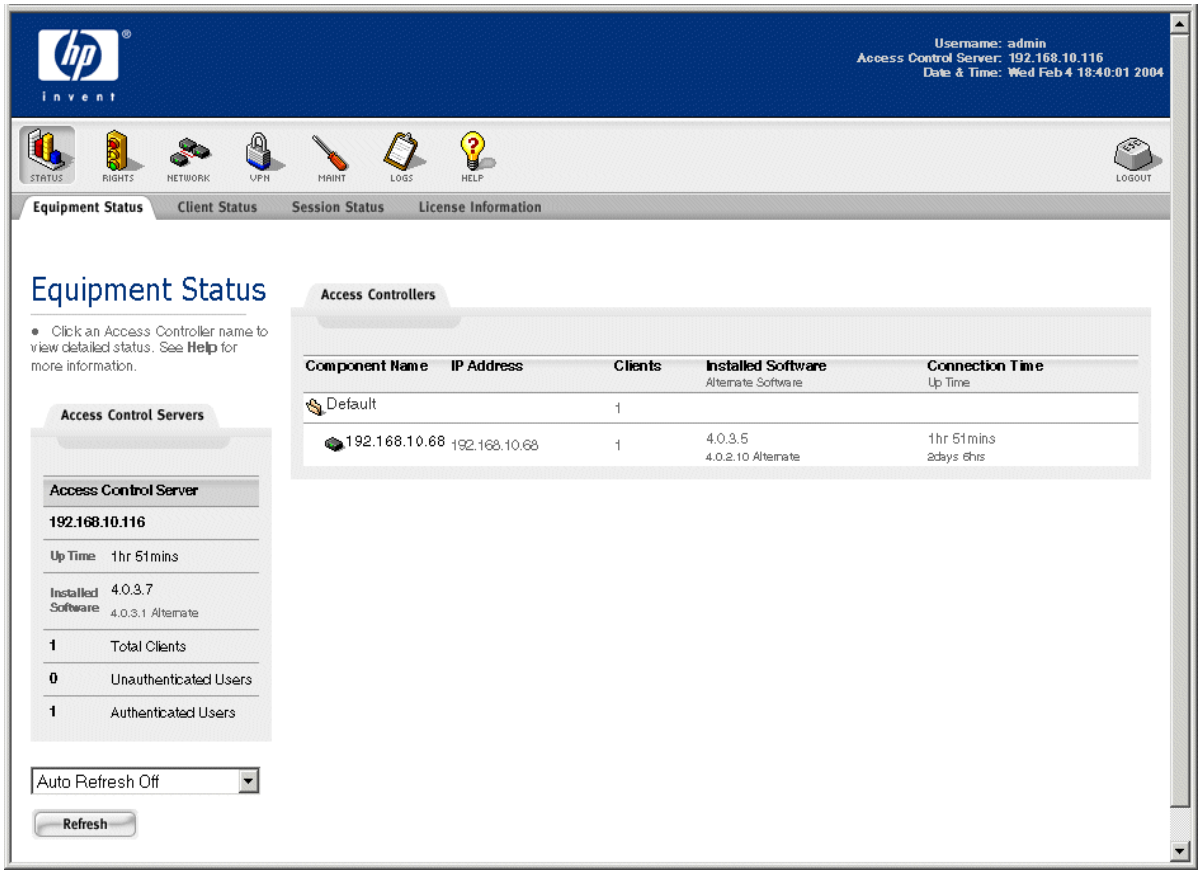
The Status Area

With the exception of the Log Files page, the functions under the Views area of the old Administrative Console are available under the Status area of the new Administrative Console.

The Equipment Status Tab (Active Access Controllers)

To view the status of 700wl Series system components (Access Control Servers and Access Controllers), click the **Equipment Status** tab under the **Status** area. See Figure 2-28.

Figure 2-28. The Status Area: Equipment Status Tab



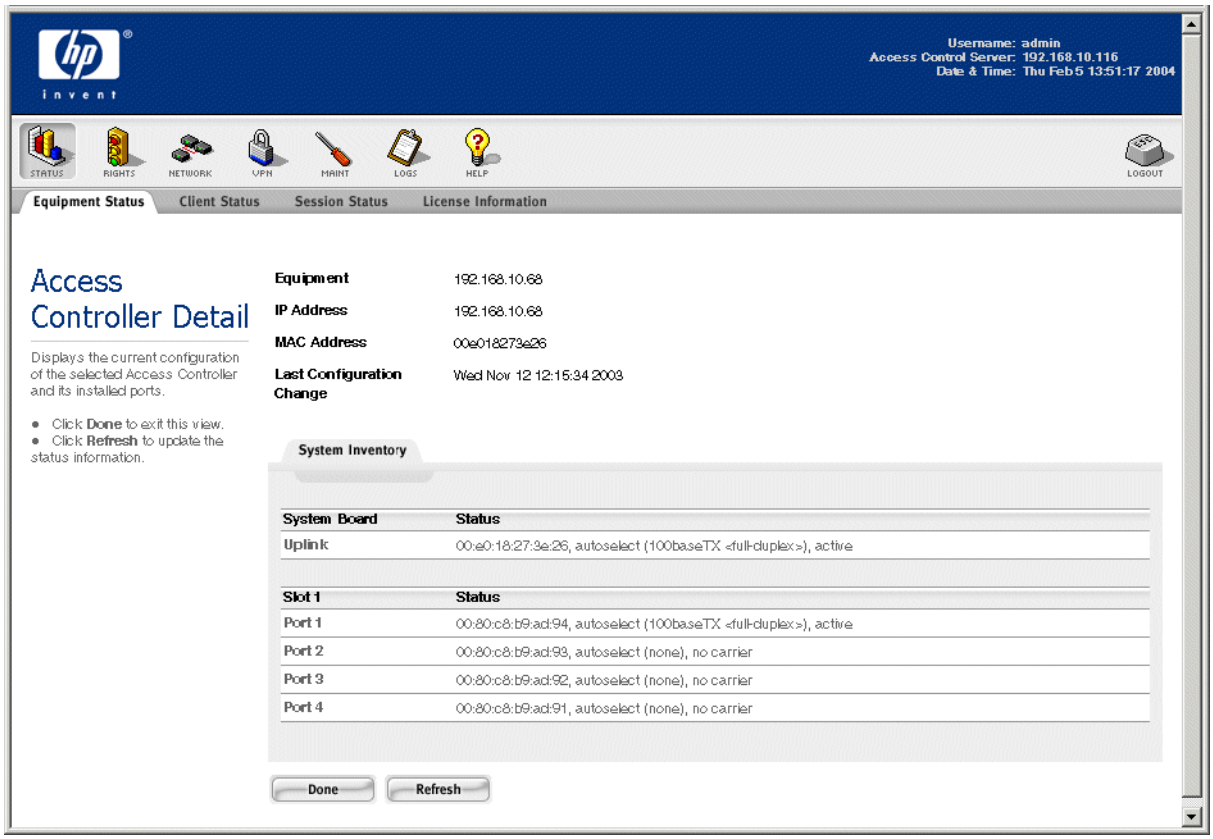
When you first logon to the Administrative Console, the **Equipment Status** tab in the status area is the first page you see.

This page shows status information for all 700wl Series system equipment. The Access Control Server status is displayed in the left panel. The Access Controller status is displayed in the right panel, using the System Components List. Open and close the folders to display just the Access Controllers of interest.

This page contains dynamic information. Select the desired data refresh interval and click **Refresh** to have the information on this page automatically refreshed.

Click on the label for an Access Controller to view detailed status information for that Access Controller. See Figure 2-29.

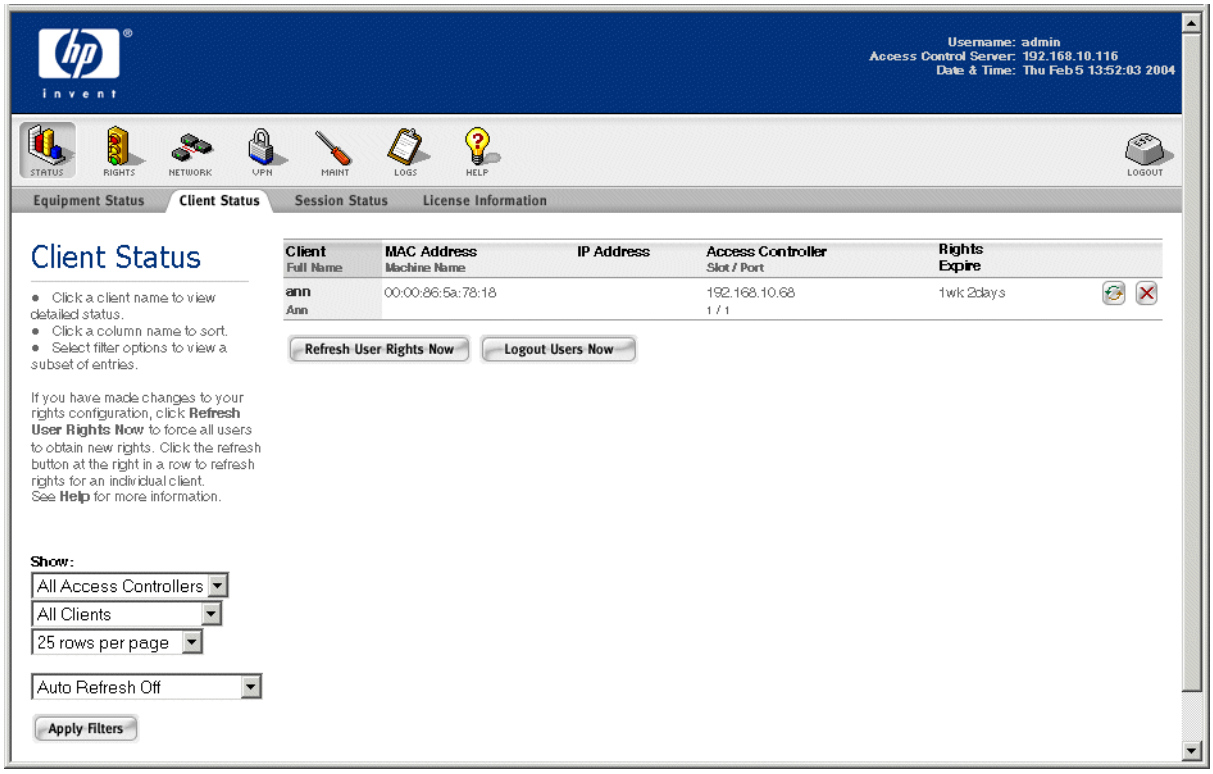
Figure 2-29. Access Controller Detail Page



The Client Status Tab (Active Clients)

To view the list of current clients attached to the 700wl Series system, click the **Client Status** tab under the **Status** area, see Figure 2-30.

Figure 2-30. The Status Area: Client Status Tab



The **Client Status** table contains the client's username, their full name (if known), the MAC address and IP address of the client's host, the location and the Access Controller to which the client is connected, the number of active sessions they are running, their idle time, and when their current rights package expires.

Links to the log information, the list of active sessions, and the Rights package information are helpful to you when troubleshooting the client's problem.

The refresh rights icon ( ) and the logout icon ( ) at the right of each client's row allows you to refresh the rights or log that client off the system.

» Click a **username** link to display the Client Information page for that user.

» Select any client filters you want to apply in the left panel of the Client Status page. You can filter by a combination of:

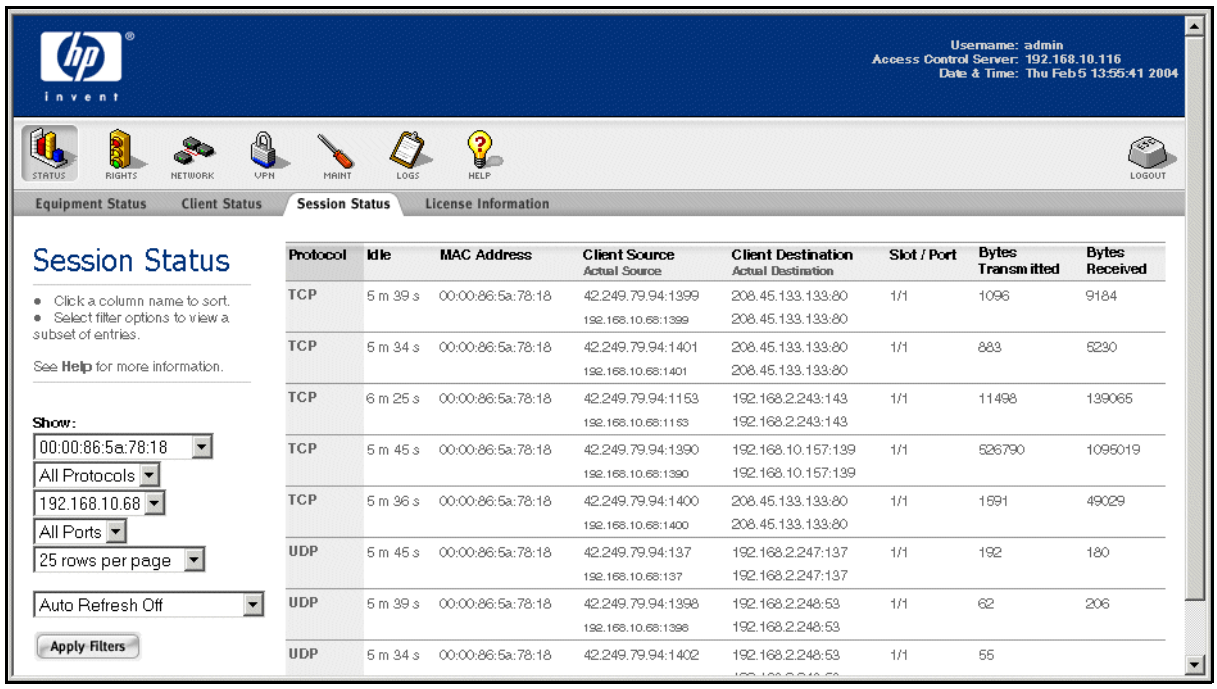
- Access Controller
- Type of client (e.g., authenticated clients, unauthenticated clients, network equipment)

» Select the desired data refresh interval and click **Apply Filters** to have the information on this page automatically refreshed.

The Session Status Tab (Active Sessions)

The Administrative Console provides two ways to display clients' activities. One is by displaying the list of active *clients*; the other is by displaying the list of active *sessions*. To view the list of active sessions, click the **Session Status** tab under the **Status** area, see Figure 2-31.

Figure 2-31. The Status Area: Session Status Tab



The session status table can be sorted by the values in any of its columns. To do this click on the column heading.

» Select any session filters you want to apply in the left panel of the Client Status page. You can filter by any combination of:

- MAC address
- Protocol being used by the client
- Port
- Access Controller

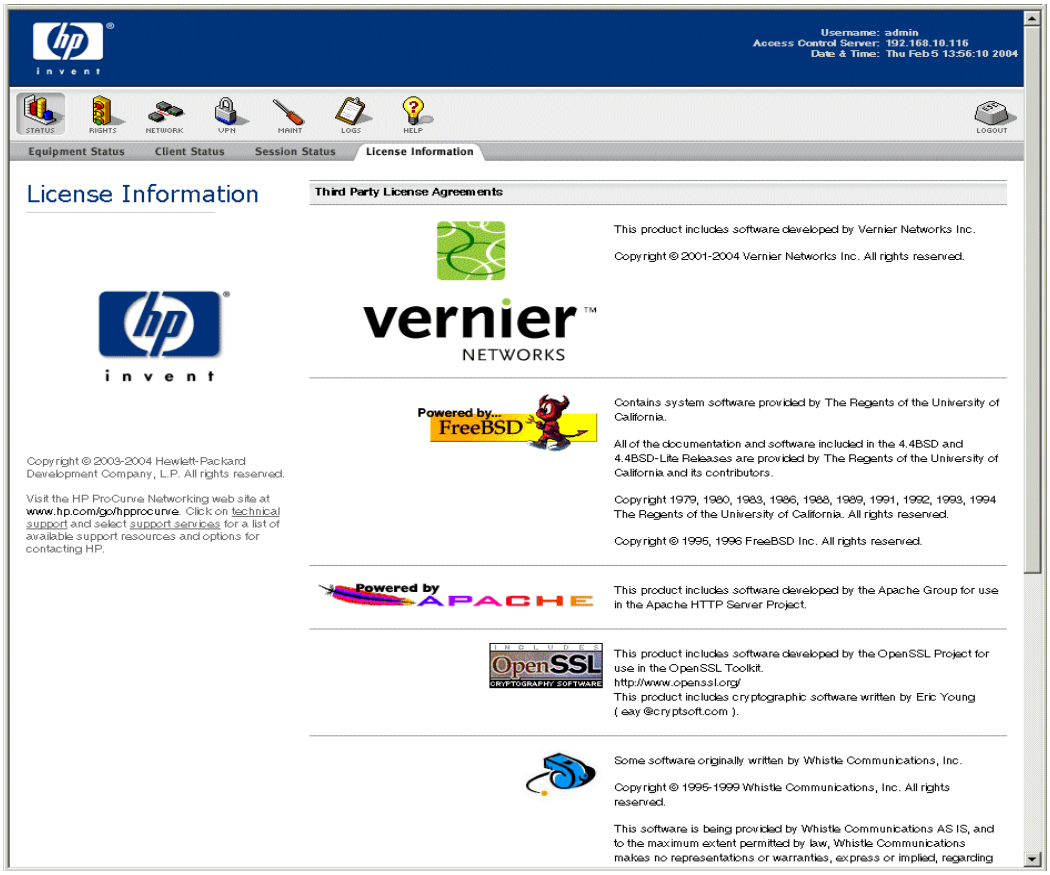
» Select the desired data refresh interval and click **Apply Filters** to have the information on this page automatically refreshed.

» Select the number of rows to display on a page in the rows/page setting pulldown. This setting is applied when you click **Apply Filters**.

The License Information Tab

To view version and license information for 700wl Series system, click the **License Information** tab, see Figure 2-32.

Figure 2-32. The Status Area: License Information



The Logs Area

The Logs area includes both the **Specify Session Logging** function from the **Configuration** area of the old **Main Menu**, and the **Log Files** function from the **Views** area.

What's Changed

- Authorization log entries and session log entries are now kept in the same place.

The Log Files Tab

To view the system logs click the **Log** icon on the Navigation bar. This displays the Log Files page. See Figure 2-33.

The Log Files page shows the system log for all the 700wl Series system equipment. The left panel provides a set of filters you can use to filter the log file.

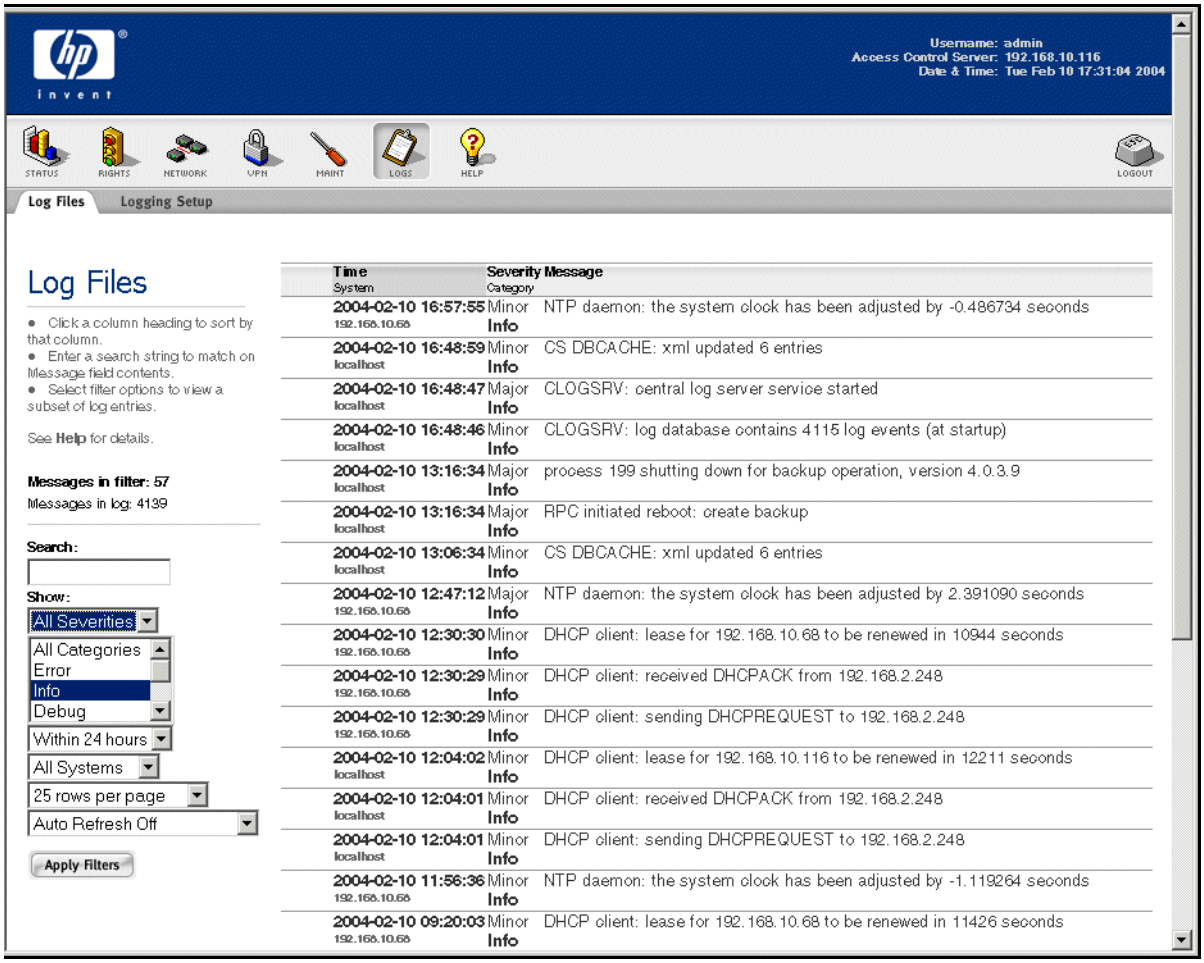
» To filter the log file, set the desired filters and click **Apply FIlters**.

» To sort the log file, click the column heading of the column on which you wish to sort: **Time**, **Severity**, or **Message** text.

» Select the desired data refresh interval and click **Apply FIlters** to apply the current filters and have the information on this page automatically refreshed.

» Selecting the number of rows to display on a page in the rows/page setting pulldown. This setting is applied when you click **Apply Filters**.

Figure 2-33. The Logs Area: Log Files Tab

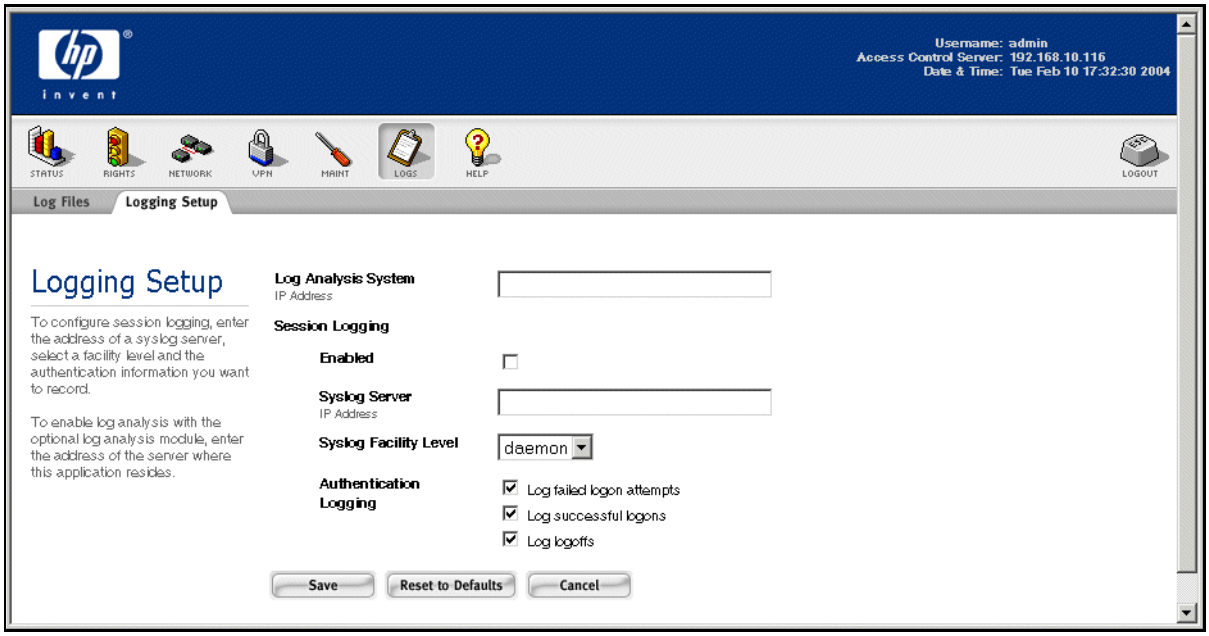


Logging Setup

To configure the settings for logging for the 700wl Series system, click the **Logging Setup** tab in the Logs area, see Figure 2-34.

Enter the logging setup information for both authorization logging and session logging on this page.

Figure 2-34. The Logs Area: Logging Setup



3

THE NEW RIGHTS MANAGER

This chapter will familiarize you with the new model for user rights in the 700wl Series system. This model is based on the previous model with which you are familiar, but has been changed to make it more intuitive and easier to manage. There have been changes in terminology, considerable changes in how you set up and manage rights (to streamline your workflow), and some changes in functionality. Read this section carefully before you start to migrate your current system to the new version.

The topics covered in this chapter include:

For a more detailed explanation of how access rights and authentication works in the new system, see chapters 4 and 5 of the *HP ProCurve Secure Access 700wl Series Management and Configuration Guide.* While working with the system, if you need further information on a particular part of the Rights Manager, consult the on-line documentation by clicking on the help icon () on the Administrative Console's Navigation bar to get context-sensitive help for the screen with which you are working.

The Rights Manager

The Rights Manager has been completely redesigned for version 4. However, most of the basic building block for specifying rights have not changed, although their names may have changed:

- Wheres—This concept has not changed, but they have been renamed *Locations*. Version 3.1 *Wheres* are automatically converted into Locations in version 4.
- Whens—This concept has not changed, but they have been renamed *Time Windows*. Version 3.1 *Whens* are automatically converted into *Time Windows* in version 4.
- Allows (both system and user-defined)—This concept has not changed. Allows are preserved during the migration process to version 4.
- Redirects (both system and user-defined)—This concept has not changed. Redirects are preserved during the migration process to version 4.
- Authentication Realms—This concept has not changed, but these have been renamed Authentication Policies. They are preserved during the migration process to version 4.
- Authentication Services—These have not changed. They are preserved during the migration process to version 4.

- The built-in database—This concept has not changed. There is a new category, Network Equipment, for devices such as Access Point, switches and the like that may appear as clients but should be handled differently in terms of authentication and rights. User entries in the built-in database are preserved during the migration process to version 4 (clients of type Access Point appear in the new Network Equipment category).
- HTTP Proxy Filters—The concept has not changed, but HTTP Proxy filters are NOT migrated automatically to version 4. If you use HTTP proxy filtering, you will need to recreate your proxy filter specifications under version 4.
- Customized Logon pages—The concept has not changed, but these pages are NOT migrated automatically. They must be recreated and linked to the appropriate Connection Profiles.

Beyond this, the way rights are handled in version 4 is quite different from version 3.1. The new rights model is conceptually much simpler and more straightforward to configure than in version 3.1. However, the higher-level rights information—the new 4 counterparts to 3.1 Groups and Locations with their various settings—must be recreated for version 4.

What's Changed

The old Groups and Locations from version 3.1 are not migrated to version 4 when the system software is upgraded. Instead, you must create Identity Profiles, Connection Profiles and Access Policies that map the functionality of your 3.1 Groups and Locations:

- The function of Groups as a collection of users has been replaced by Identity Profiles
- The function of Groups as the definition/specification of access control has been replaced by Access Policies
- 3.1 Locations have been replaced by Connection Profiles
- Authentication Realms have been migrated to Authentication Policies, which are in turn linked to Connection Profiles
- The method by which precedence was determined for Redirect filter evaluation has changed. In version 3.1, Redirects (and Allows) were evaluated based on the alphabetical ordering of their names. Thus naming was important to ensure that Redirects were evaluated in the correct order. In the new version, you can explicitly reorder the evaluation of Redirect filters by changing their position in the Redirect filters list. You can name them anything you want.
- Customized logon pages are now linked to Connection Profiles. They must be recreated in version 4.
- The process for determining what rights apply to a client at any given time is quite different.
- HTTP Proxy Filter settings are not preserved after an upgrade to 4. You must recreate your filter specifications. HTTP proxy filtering is now configured as part of an Access Policy.

New Rights Manager Concepts and Terminology

The following sections define the key new concepts of the new Rights model implemented in version 4.

Connection Profiles

In the old Rights Manager, a Location was a combination of a set of "Wheres" that specified a physical location or set of locations defined as Access Controller ports. The Location also included other attributes that are not logically connected with the common idea of a location, including:

- A set of "Whens" to control when access is allowed through the Location.
- A set of "Groups" to control who is allowed access through the Location.

The old Location concept also included settings for whether client addresses should be NAT'ed, and whether VLAN tags should be added to packets entering through the location. In addition, security settings (whether to require encryption) were based on the Location.

The new Rights Manager introduces the ***Connection Profile*** to replace the old concept of Location. A Connection Profile is used to classify clients based on the characteristics of how they connect to the network. Like a version 3.1 Location, a Connection Profile specifies both the physical entry point (a *Location* as a set of Access Controller ports) and the time (*Time Window*) of the connection. In addition, it allows you to specify a VLAN tag as a further characteristic of the Connection Profile. When a client connects to the network, that client is associated with a Connection Profile based on whether it matches the Connection Profile characteristics in terms of Access Controller ports, time of day, and VLAN tag, if any.

The Connection Profile has two uses:

- The Connection Profile specifies how a user is authenticated when they connect to the system. Each Connection Profile is associated with a ***Authentication Policy*** (an ordered set of *Authentication Services).* Authentication Policies are equivalent to Authentication Realms in a version 3.1 system, except that they can also include NT Domain Logon and 802.1x Logon as "services" rather than using a whole separate configuration scheme to specify those authentication methods.
- The Connection Profile is used, along with the Identity Profile, to determine the Access Policy that applies to the client, where the Access Policy defines the set of access rights granted to the client.

Where in version 3.1 the Location determined what encryption protocols were allowed or required, and whether NAT would be required, in version 4 these are determined by the Access Policy that applies to the client, which is determined by the combination of Connection Profile and Identity Profile that a client matches.

Identity Profiles

In the old Rights Manager a Group was the combination of a set of clients (users or access points) plus a set of access rights for that set of clients. The group also included a set of "whens", so that "whens" appear both as part of a location (where they constrain when a connection can be made) and as part of a group (where they constrain when the group's set of rights are valid).

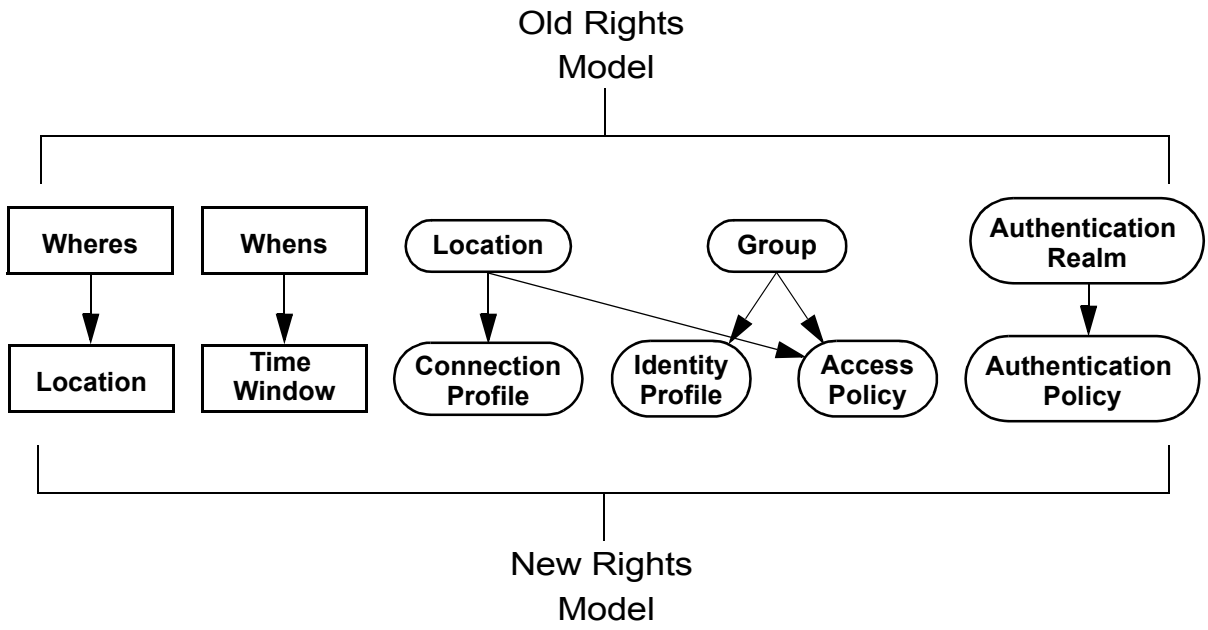
This made the *group* concept confusing since it combined the normal idea of a group (a set of clients) with the Access Policy for the members of that group, and a time window. This was further complicated by the idea of a group type (Guest, Logon, Implicit User, Normal, Access Point, and Stop). The group types mapped onto basic sets of access rights.

The new Rights Manager replaces the concept of a group with two new terms—***Identity Profile*** and ***Access Policy***. This allows the separation of the *who* part of a group (the set of clients) from the *what* part (*what* the users are allowed to do on the network). Making this separation allows the Rights Manager to dispense with the group type.

There are no time windows in an Identity Profile. An Identity Profile is simply a set of clients. These can be users who log onto the system or access points. Access points are now called ***Network Equipment***.

These changes in concepts and terminology are summarized in Figure 3-1.

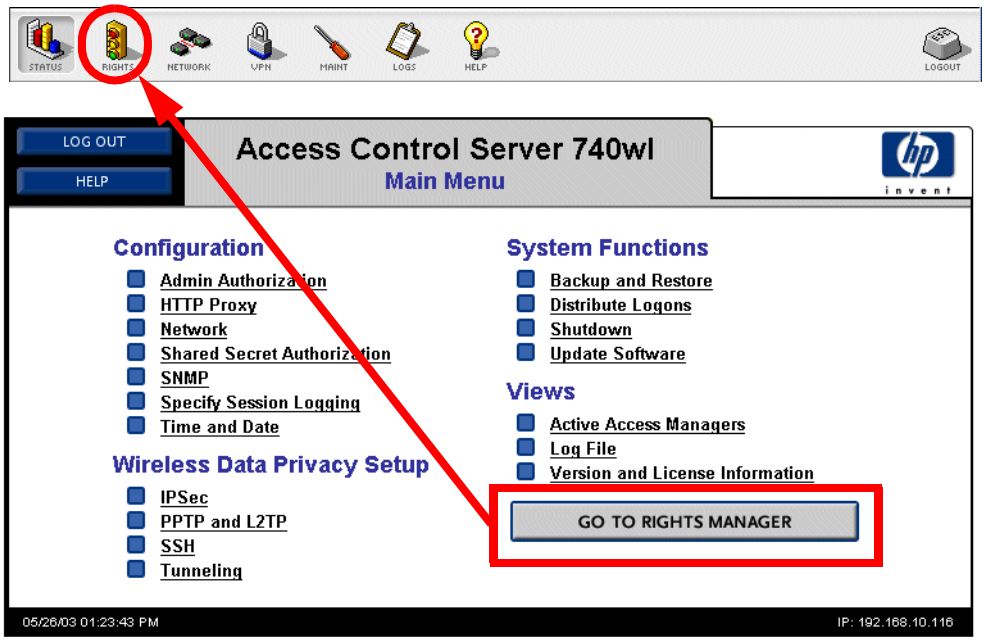
Figure 3-1. How the Old Rights Concepts Map to the New RIghts Concepts



The 700wl Series System Management and Configuration Guide provides a more detailed explanation of how to work with the new Rights Manager.

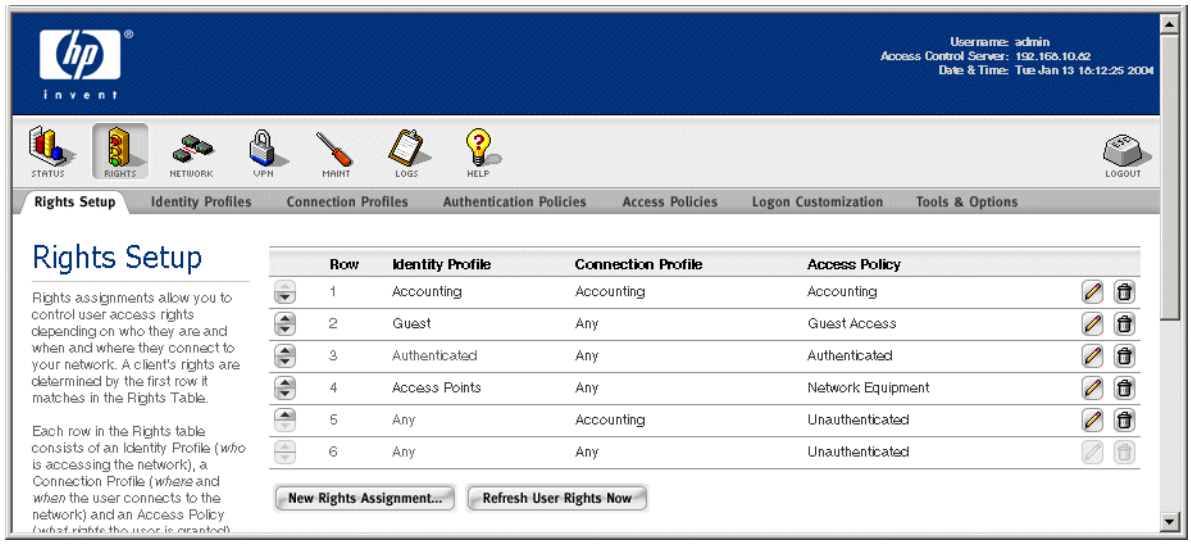
» To access the new Rights Manager, click the **Rights** icon on the Navigation bar. See Figure 3-2.

Figure 3-2. Where to Find the Rights Manager



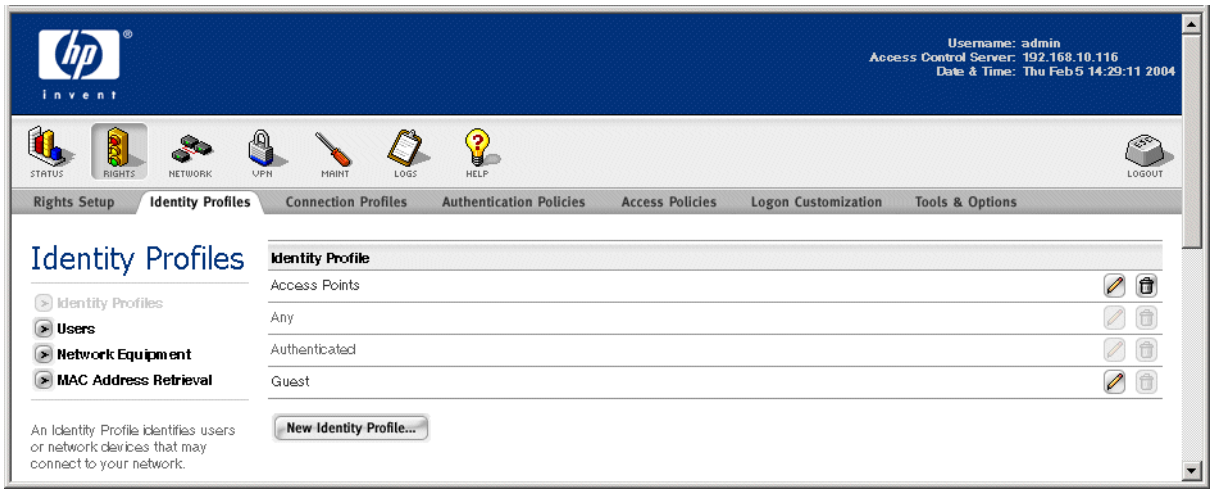
Once the proper *Identity Profiles*, *Access Policies*, *Authentication Policies*, *Locations*, *Time Windows*, and *Connection Profiles* are created, rights are maintained and managed with the Rights Assignment table. To go to the Rights Assignment table click the **Rights Setup** tab in the Rights Manager. See Figure 3-3.

Figure 3-3. Rights: Rights Assignment Table



To set up Identity Profiles, click the **Identity Profiles** tab in the Rights Manager. See Figure 3-4.

Figure 3-4. Rights: Identity Profiles Table

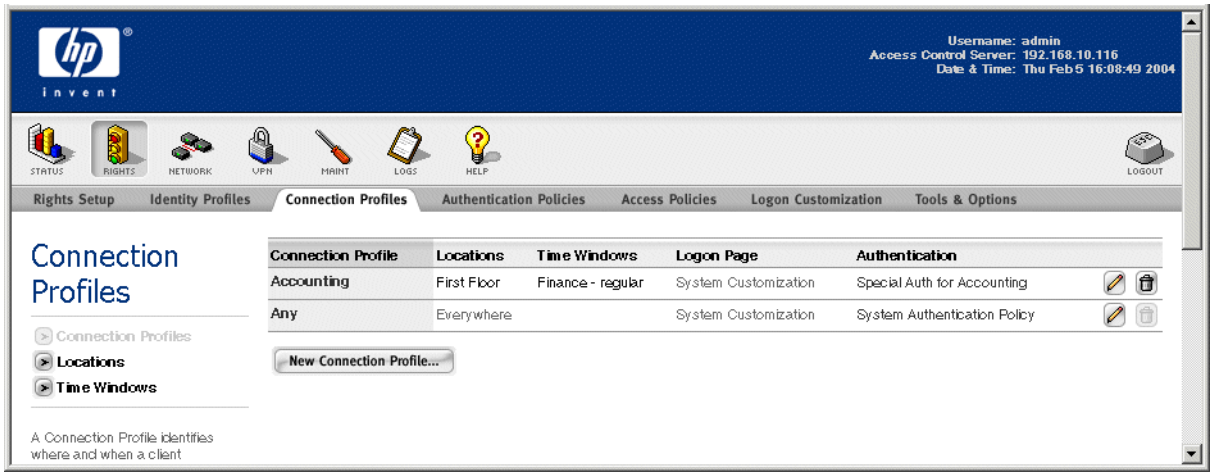


To set up *Connection Profiles* click the **Connection Profiles** tab in the Rights Manager. See Figure 3-5. This page initially displays the Connection Profiles table. From this page you can also go to the Locations page, to set up or edit locations, and the time windows page to set up or edit time windows.

» To set up or edit *Locations* click the **Locations** link in the left panel of the Connection Profiles page. See Figure 3-4.

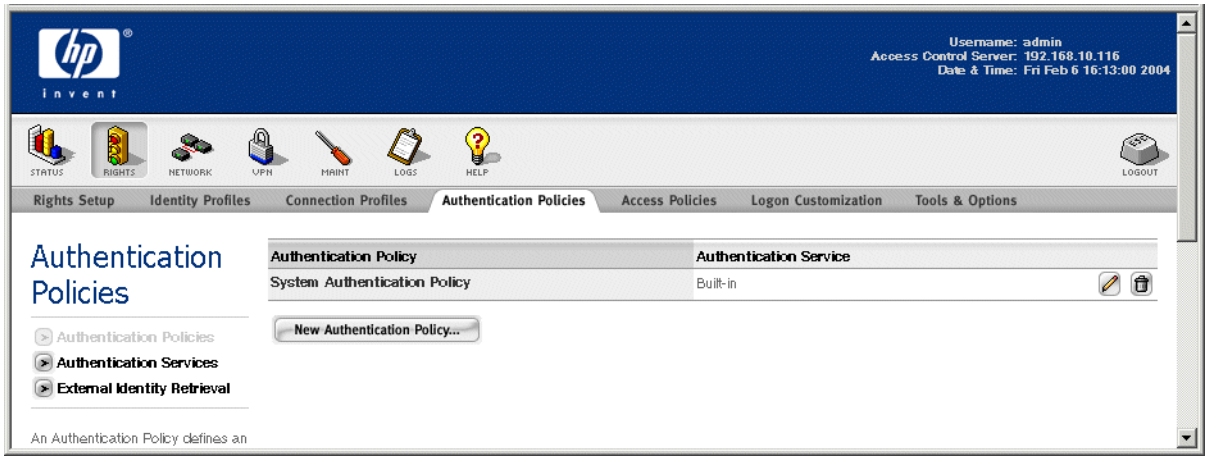
» To set up or edit *Time Windows* click the **Time Windows** link in the left panel of the Connection Profiles page. See Figure 3-5.

Figure 3-5. Rights: Connection Profiles Table



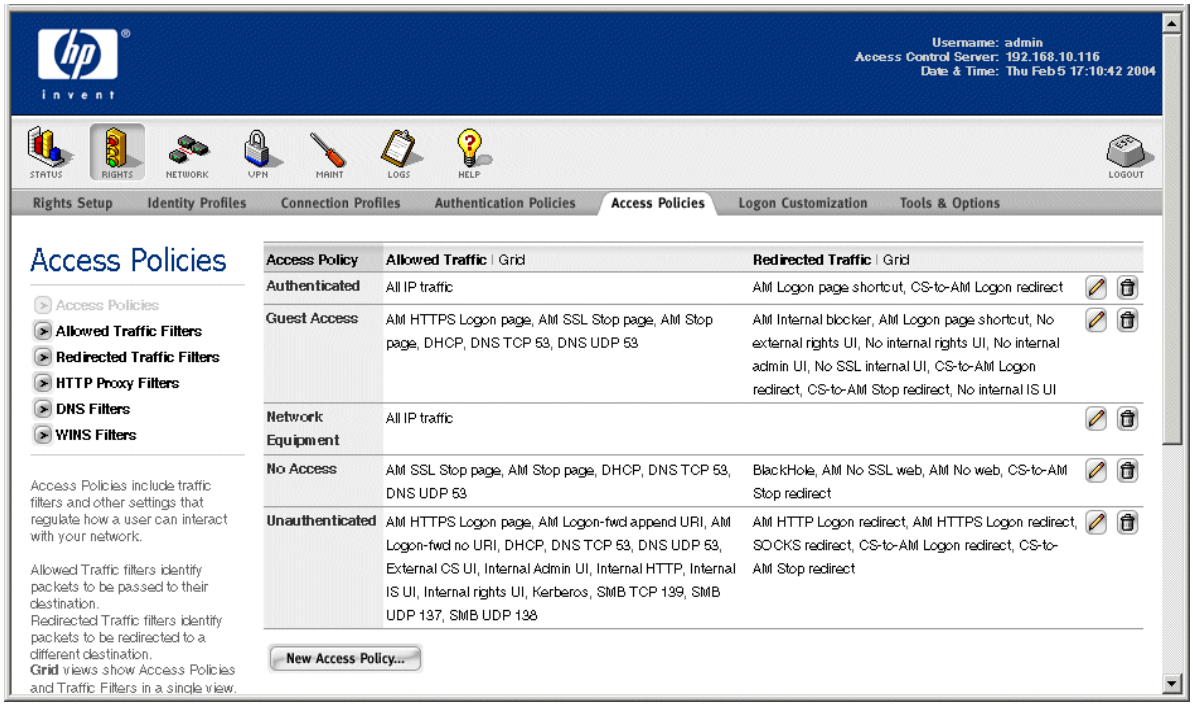
To set up Authentication Policies, click the **Authentication Policies** tab in the Rights Manager. See Figure 3-6.

Figure 3-6. Rights: Authentication Policies Table



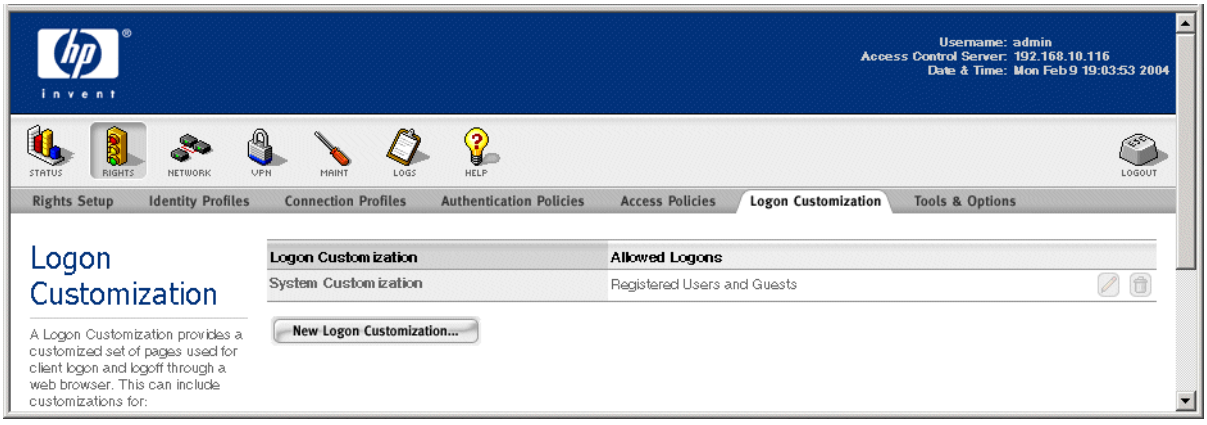
To set up *Access Policies* click the **Access Policies** tab in the Rights Manager. See Figure 3-7.

Figure 3-7. Rights: Access Policies Table



To set up *customized logon pages* click the **Logon Customization** tab in the Rights Manager. See Figure 3-8.

Figure 3-8. Rights: Logon Customization Table

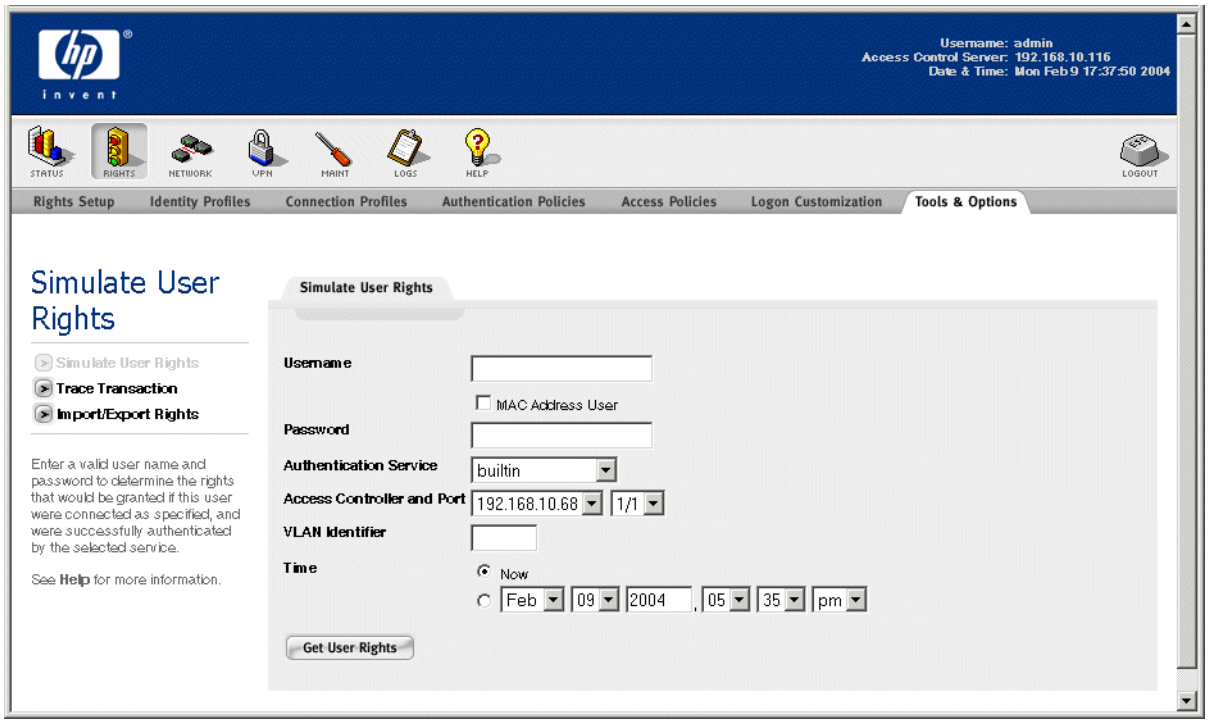


The 700wl Series system provides tools to help with verifying and troubleshooting rights settings. These tools are:

- A rights simulator that shows what rights a user would have.
- A tracer to troubleshoot Authentication Service Transactions
- The ability to export and import rights in an XML format (which is also human readable)

To use the right area tools click the **Tools & Options** tab in the Rights Manager. See Figure 3-9. This initially displays the **Simulate User Rights** page.

Figure 3-9. Rights: Tools & Options



» To use the authentication transactions tracer click the **Trace Transactions** link in the left panel of the Simulate User Rights page. See Figure 3-9.

» To export or import rights click the **Import/Export Rights** link in the left panel of the Simulate User Rights page. See Figure 3-9.

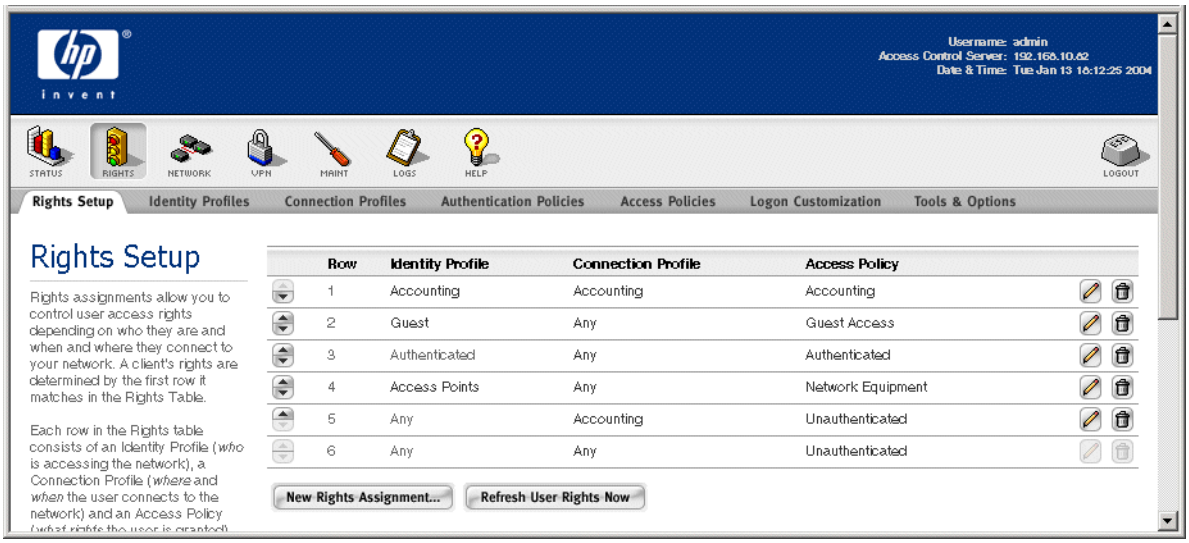
Access Rights in the 700wl Series system

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 (the Access Controller port through which the client is connected), the current time, 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 3-10).

Figure 3-10. Rights Assignment Table



When a client connects to the 700wl Series system, the Rights Manager 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, as known to the system, or location changes, the Rights Manager matches the client to an Identity Profile and to a Connection Profile, and then searches the Rights Assignment table to determine the Access Policy appropriate for that combination of Identity Profile and Connection Profile.

For example, when a client first connects to the system, it typically does not match any of the explicit Identity Profiles. However, the client always will match the built-in Identity Profile called *Any*. All clients, by definition are members of the *Any* Identity Profile. Similarly, all clients will match the built-in Connection Profile called *Any*, even if they do not match any of the explicit Connection Profiles.

When the Rights Manager searches the Rights Assignment table, the search 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 chapter 5 of the *700wl Series system Management and Configuration Guide* for a complete 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 an explicit Identity Profile (for example, the "Authenticated" profile). The client 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 matches a different row in the Rights 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 New Rights Manager

Note: *To be able to use the new Rights Manager you must have the correct Administration Level set in your User profile in the 700wl Series system. You must have an Administration Level setting of either Console Administrator or Rights Administrator (see the discussion of admin levels on page 3-11).*

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

Figure 3-11. The Rights Icon on the Navigation Bar

Within the Rights Manager you may perform any of the following tasks:

- 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
- Customizing the Logon page (and other associated pages) presented to users whose first network access attempt is an HTTP request.
- Creating new rows in the Rights Assignment Table

As a part of creating and modifying these profiles and policies, you can also define the following:

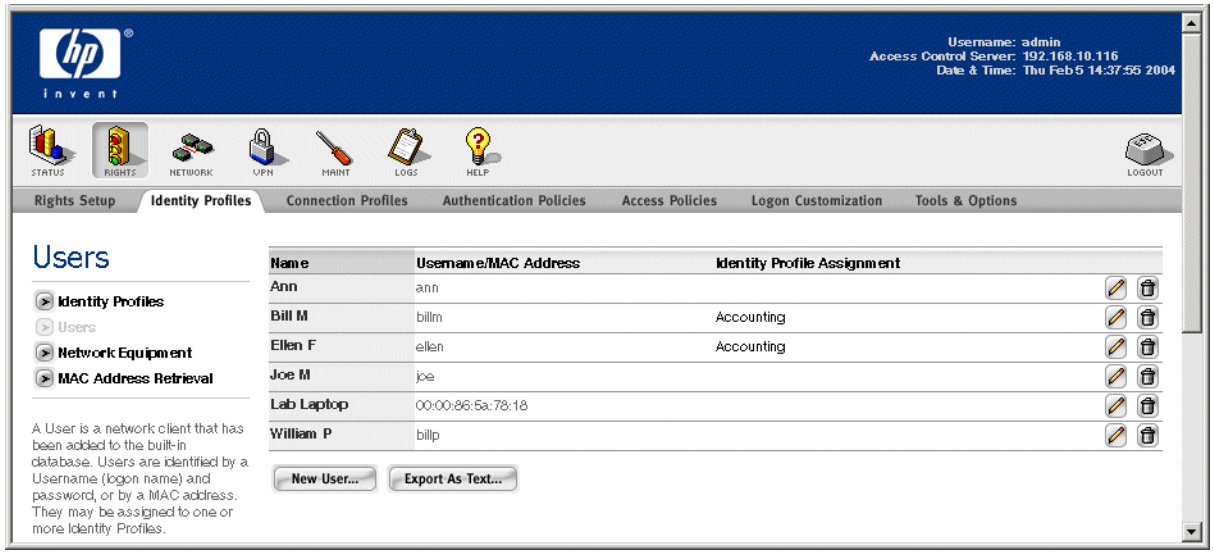
- *Users* (defined by a username and password) and *Network Equipment* (defined by a MAC address) to be included in the built-in database. These may be used when defining an Identity Profile.
- *Locations* (defined as a set of one or more ports on one or more Access Controllers). These may be used when defining Connection Profiles.
- *Time windows* (defined as a range of hours, dates, or days of the week). These may be used when defining Connection Profiles.
- *Allowed Traffic Filters* and *Redirected Traffic Filters*. These may be used when defining Access Policies.
- *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, import a set of stored Rights from the local system, and download the XML schema that defines the format of the Rights definition file.

Configuring Access Rights—An Overview

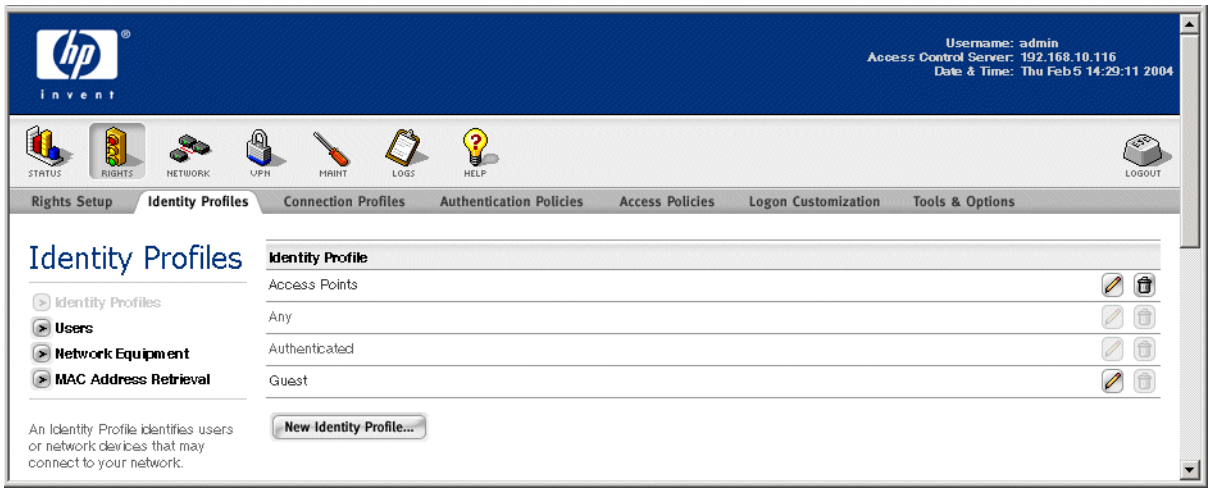
To configure rights in the 700wl Series system, you first need to decide how you want to control access to the resources on your network.

Figure 3-12. The Rights Manager: Users Page



Step 1. *Add Users* to the 700wl Series system built-in database. Users are automatically migrated from your 3.1 system to version 4 as part of the upgrade process.

Figure 3-13. The Rights Manager: Identity Profile Page



Step 2. *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 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.

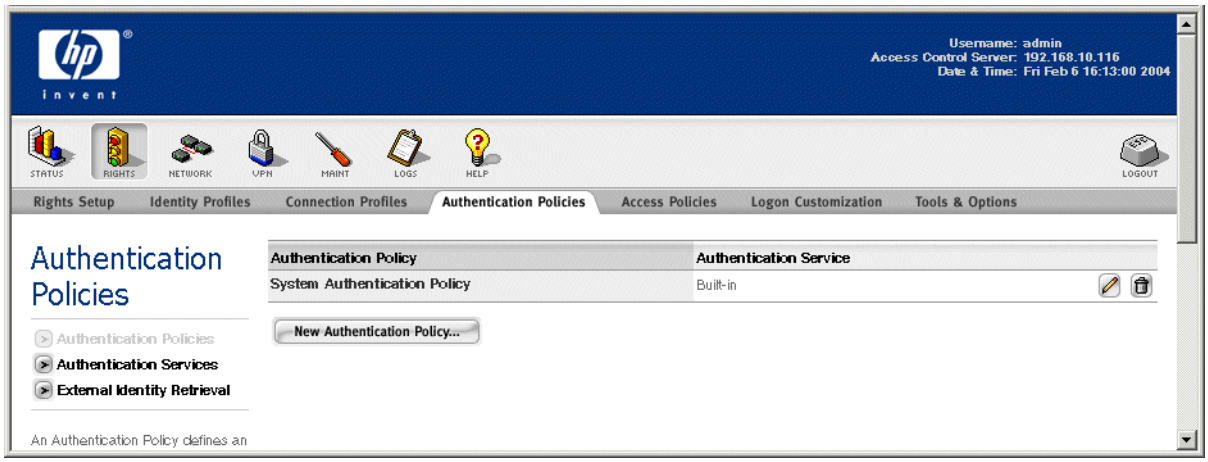
You add users to the 700wl Series system built-in database and then assign those users to Identity Profiles through the Rights interface, or you can define Identity Profiles that match users based on group or domain information retrieved when the user is authenticated. You can add clients to the 700wl Series system built-in database based on their MAC address as well. These machine clients are termed network equipment; they include the system access points.

If the MAC address data for the network equipment is available from a remote service (for instance from an LDAP server), you can retrieve the data automatically using the *MAC Address Retrieval* feature of the Rights Manager.

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.

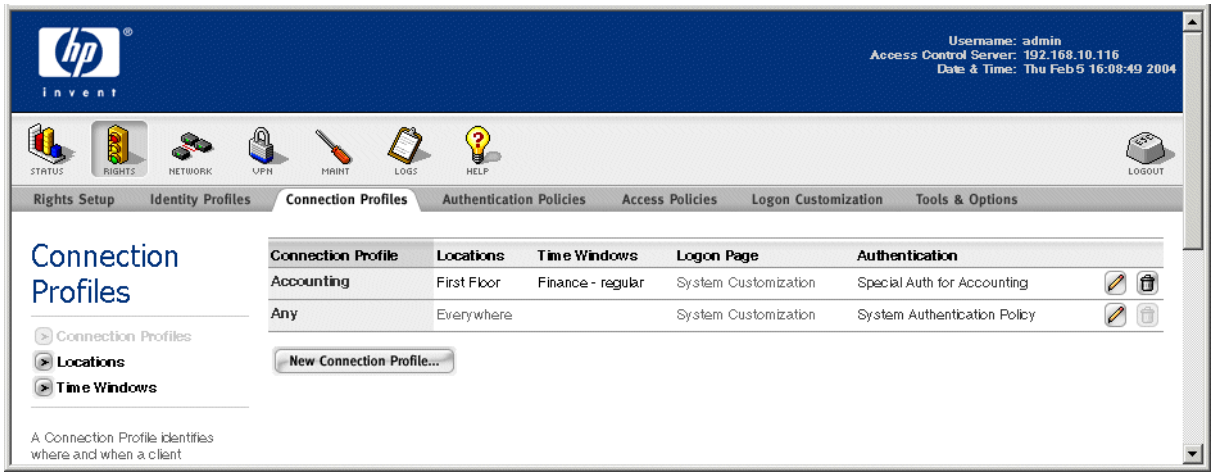
b. *Add network equipment* (such as Access Points) to the built-in database so they can be assigned a set of access rights — for example, to allow the device to be managed over the network.

Figure 3-14. The Rights Manager: Authentication Policy Page



Step 3. *Create Authentication Policies* to provide different protocols for how a user is authenticated when he connects to the system. An ***Authentication Policy*** is an ordered set of Authentication Services (such as a specific LDAP server, RADIUS server, Kerberos server, XML-RPC service or the 700wl Series system built-in database) used to establish the identity of the user. (Authentication Policies are equivalent to Authentication Realms in the old system and are automatically migrated from your 3.1 system as part of the upgrade to version 4.)

Figure 3-15. The Rights Manager: Connection Profile Page



Step 4. *Create Connection Profiles* to differentiate between physical locations where clients can access the system, or adjust access based on the time of day or days of the week, *etc.*, or to differentiate between clients on different VLANs, or a combination of all three. This differentiation can be used to assign different access rights, or to use different authentication methods to verify the identity of the user, or both.

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

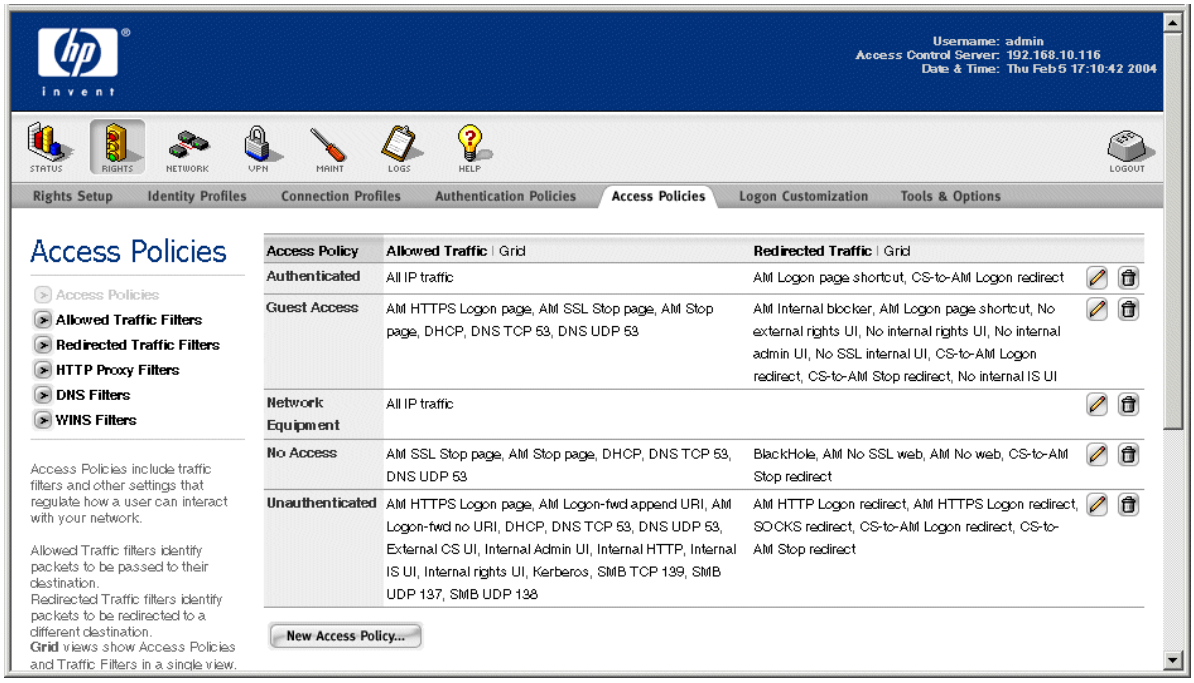
For example, do you want students to get different access rights while they are in the Library from those they get in a science lab? Do you want clients connecting from your Corporate Visitors Center to be authenticated differently from clients connecting from your manufacturing floor? You can use locations to define Connection Profiles that are unique to a specific physical location—a building, a department, a floor, a conference room.

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 (these are automatically migrated over from the *wheres* and *whens* of your 3.1 system). 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.

Figure 3-16. The Rights Manager: Access Policy Page



Step 5. *Create Access Policies* that define the sets of access rights you want to grant based on a client's Identity Profile and Connection Profile.

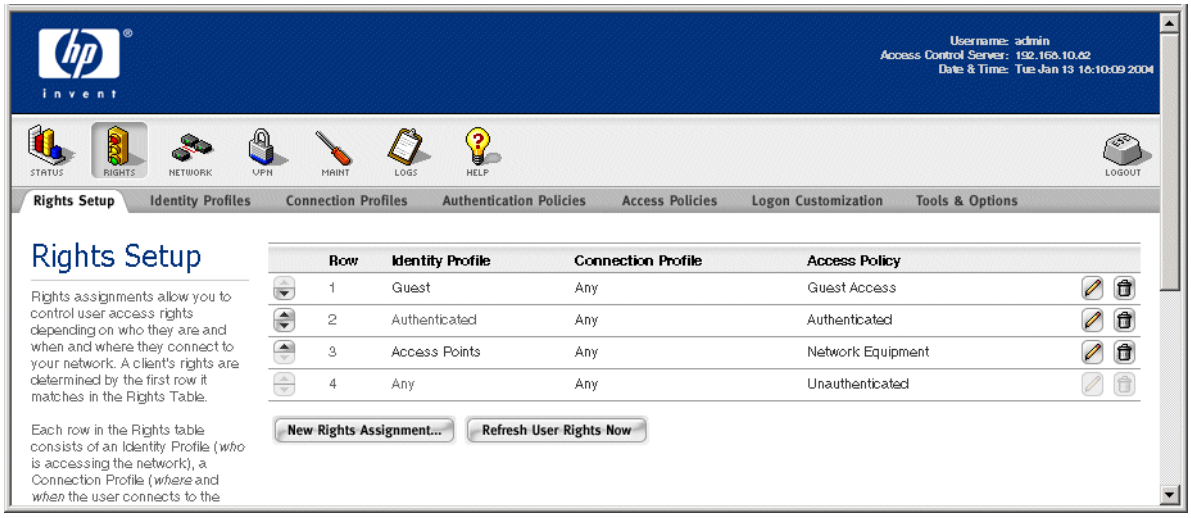
You can create as many Access Policies as you need. Each row in the Rights table can have a different Access Policy, meaning you can create a different policy for every combination of Identity and Connection Profiles, if needed.

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 which 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.

a. *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 want 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.

Figure 3-17. The Rights Manager: The Rights Assignment Table Page



Step 6. *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.

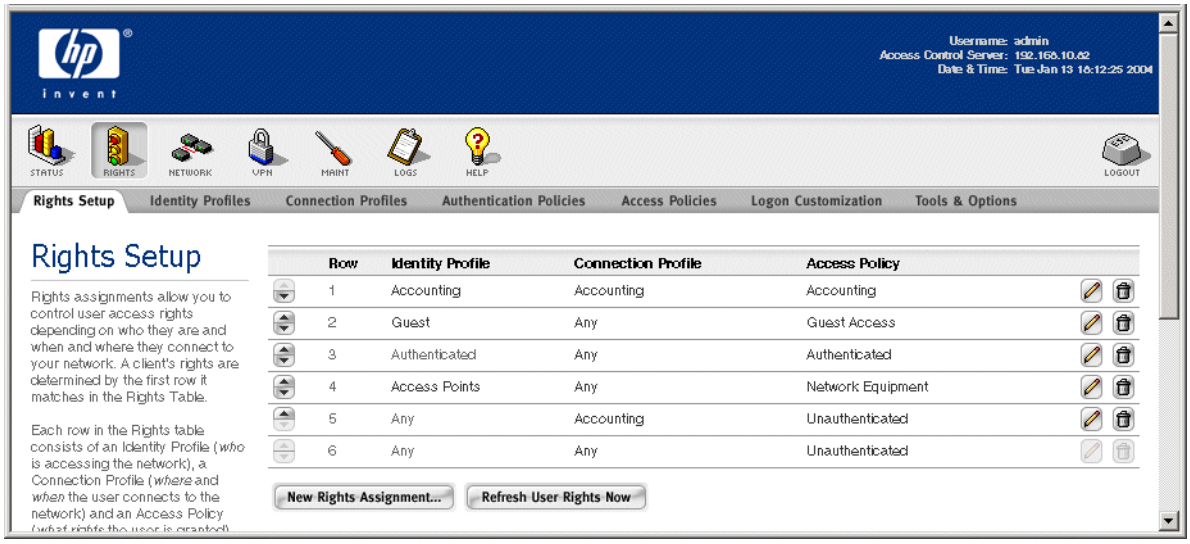
Using the Rights Assignment Table: Examples

To understand how the Rights Assignment Table is used by the 700wl Series system, consider the following examples, based on the Rights Assignment Table shown in Figure 3-18. 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 700wl 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 700wl Series system, the client does not match the Identity Profiles in the first four rows, it falls through to the bottom two rows of the table, where it automatically matches the "Any" Identity Profile. If the client accessed the 700wl Series system through a physical location that matches the Connection Profile "Accounting Department," it matches 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.

Figure 3-18. Rights Assignment Table



Step 3. Given the rights defined by the "Unauthenticated" Access Policy, when the client attempts to access any web page, he/she is instead redirected to the 700wl 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 are passed on for authentication based on the Authentication Policy 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.

If the user enters a logon name and password that is authenticated successfully by the Authentication Policy, the 700wl Series system searches the Rights Assignment Table again using the new identification information. The user now matches 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 2.
- A client that initially matches on row 6, and is successfully authenticated, also gets new rights based on row 2. Due to its Connection Profile it does not match row 1 (and most likely it also does not match the Identity Profile "Accounting").
- If the user elects to logon as a Guest, he or she is automatically associated with the "Guest" Identity Profile, matches on row 3 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 Department" 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 Department" 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 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 "APs" 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 "APs" 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. Also, it is important that rows with the "APs" 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 "APs" Identity Profile.

Rights Manager Changes in Version 4: Summary

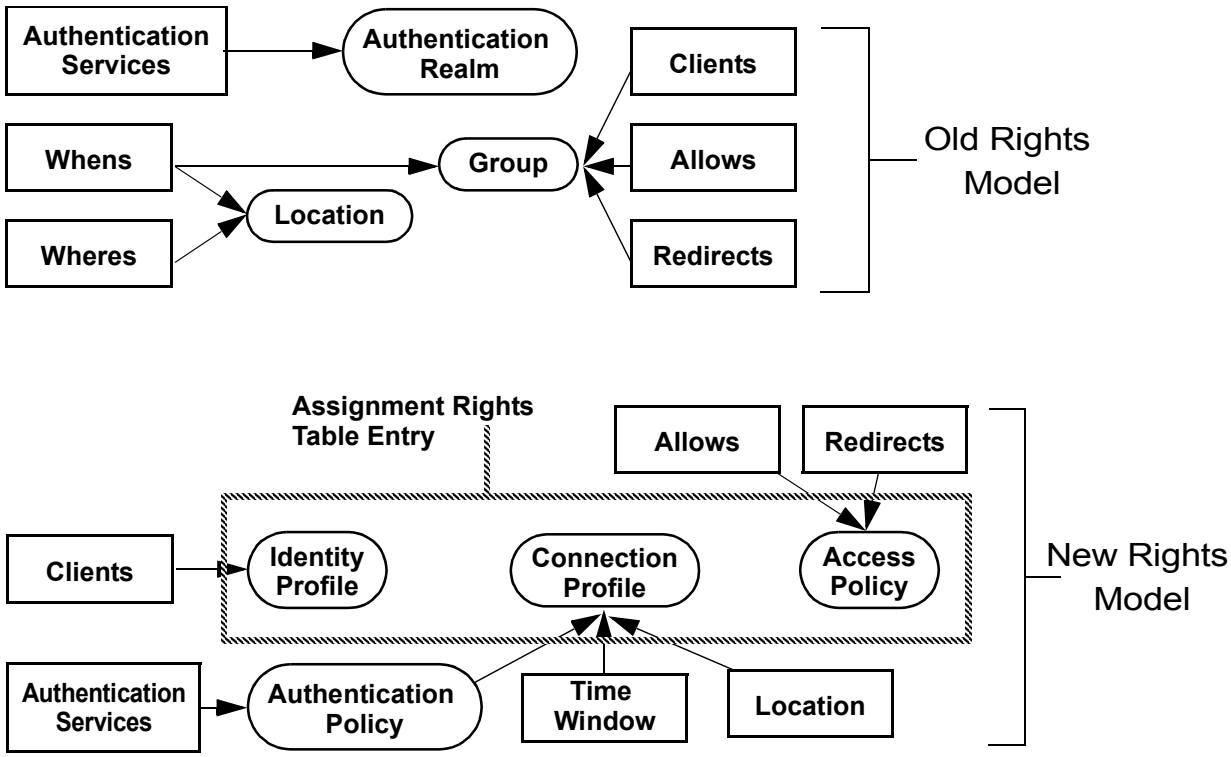
The following table summarizes the changes from version 3.1 to version 4 of the 700wl Series system in terminology associated with the Rights Manager. Terms are listed alphabetically, based on the version 3.1 term or phrase.

Version 3.1 Term/Phrase	Version 4 Term/Phrase
Access Point	Network Equipment
Allows	Allowed Traffic Filters
Authentication Realm	Authentication Policy
Client Probes	Client Polling
Disassociate clients after	Start linger timer after
Group *(as set of rights: allows, redirects, Real IP/NAT etc.)*	Access Policy
Group *(as a collection of "users")*	Identity Profile
• Access Point Group	• "Any" Identity Profile + "Network Equipment" Access Policy
• Guest Group	• "Guest" Identity Profile + "Guest" Access Policy

Version 3.1 Term/Phrase	Version 4 Term/Phrase
• Logon Group	• “Any” Identity Profile + “Unauthenticated” Access Policy
• Stop Group	• “Any” Identity Profile + “No Access” Access Policy
• Implicit User Group	• “Authenticated” Identity + “Authenticated” Access Policy
Location	Connection Profile
• “Everywhere Else” Location	• “Any” Connection Profile
Redirects	Redirected Traffic Filters
When	Time Window
Where	Location

Figure 3-19 provides a picture of how the relationships among these concepts have changed from version 3.1 to version 4 of the 700wl Series system.

Figure 3-19. The Old vs. The New Rights Manager Model



FUNCTIONALITY CHANGES

A

This Appendix provides a summary of the functionality changes from 700wl Series software version 3.1 to version 4.

Changed Terminology

Version 3.1 Term/Phrase	New Term/Phrase
Allows	Allowed Traffic Filters
Authentication Realm	Authentication Policy
Client Probes	Client Polling
Disassociate clients after	Start linger timer after
Group *(as set of rights: allows, redirects, Real IP/NAT etc.)*	Access Policy
Group *(as a collection of "users")*	Identity Profile
• Access Point Group	• "Any" Identity Profile + "Network Equipment" Access Policy
• Guest Group	• "Guest" Identity Profile + "Guest" Access Policy
• Logon Group	• "Any" Identity Profile + "Unauthenticated" Access Policy
• Stop Group	• "Any" Identity Profile + "No Access" Access Policy
• Implicit User Group	• "Authenticated" Identity + "Authenticated" Access Policy
Location	Connection Profile
• "Everywhere Else" Location	• "Any" Connection Profile
Redirects	Redirected Traffic Filters
When	Time Window
Where	Location

Changed Functionality

- In 3.1, redirects and allows were evaluated based on the alphabetical ordering of their names. Thus naming was important to the order of evaluation of redirects. In version 4 you can order redirect filters by moving them in the list, thus you can call them anything you want.
- All logs are stored in a single location, accessible via the Administrative Console on the Access Control Server.

- Access Controllers can be named and the name of the Access Controller is used in all displays. You no longer need to remember the IP Address of each Access Controller.

Version 4 Functionality

- Enhanced SNMP interface. Version 4 MIBs have been added:
  - — New 64-bit counter support for high speed interfaces in IF MIB - RFC 2863
  - — A HP Systems MIB that provides information on product type, software version, SNMP notifications, and environmental statistics
  - — A HP-IF-EXT MIB that provides information for each interface on the number of active clients, roaming events, and the number of current sessions
  - — A HP MEMPROC MIB that provides statistics overall product load (both CPU and memory use)

  700wl Series system version 4 has added a new SNMP trap:
  - — A failover trap—If the secondary Access Control Server becomes the primary Access Control Server (failover) that Access Control Server issues a failover trap.
- Access Control Server Redundancy (failover): 700wl Series system now supports having a secondary Access Control Server that automatically takes over if the primary Access Control Server fails.
- Bandwidth management: version 4 provides the ability to limit the bandwidth available to each client. Bandwidth can be limited differently for each Access Policy. Separate limits can be set for upstream and downstream bandwidth.
- Multiple Administrative Console access levels: version 4 allows for three different levels of access to the Administrative Console.
- Extended authentication support for VPN clients: 700wl Series system version 4 can interoperate with VPN clients from vendors that require or allow Extended Authentication (XAUTH) to establish a VPN connection. Version 4 also allows VPN clients that use XAUTH to be authenticated to the 700wl Series system during establishment of the VPN connection. Without XAUTH, VPN client users would need to authenticate using the web page after bringing up the VPN connection.

  VPN clients that are authenticated to the 700wl Series system using XAUTH are logged off when the VPN connection is terminated.
- Enhanced VLAN Support: 700wl Series system version 4 supports VLAN tagging. When an Access Controller forwards a DHCP request for a client that is being VLAN tagged going upstream, the Access Controller now tags the DHCP request with the VLAN of the client.

B

FUNCTION MAP: VERSION 3.1 TO VERSION 4

This Appendix is a summary of where in the version 4 Administrative Console to find each feature or function in version 3.1 of the for 700wl Series system. For an overview of how the version 4 Administrative Console is organized and where to find each feature, see "New User Interface" on page 1-1.

The features are grouped as they were in version 3.1 of the for 700wl Series system. The major functional areas are:

In each section the functions are listed in tabular format. The new location is shown as a series of menu or button selections that take you from any page in the version 4 Administrative Console to the page for that function. For example, the path to get to the setup page for network bridging is shown as: **Network ⇨ Network Setup ⇨ Advanced Setup ⇨ Bridging**. That is a shorthand means of saying:

Step 1. Click the **Network** icon on the Navigation bar at the top of the page. (Each path specified always starts with one of the icons on the Navigation bar at the top of the page.)

Step 2. When the new page appears, click on the **Network Setup** tab.

Step 3. When the new page appears, click on the **Advanced Setup** tab.

Step 4. When the new page appears, go to the **Bridging** section of the page.

In some cases you need to select a specific Access Control Server or Access Controller or other item; this takes you to the page of editing the setting for that item. This is shown by putting the item in angle brackets and italics. This means that you click the desired item of that type. In such cases you can also click the **New <*Item*>** button to create a new instance of the item, rather than editing the information for an existing instance. For example:

Network ⇨ System Components ⇨ *<Access Control Server>* **⇨ Enable SSH command line interface.** That means:

Step 1. Click the **Network** icon on the Navigation bar at the top of the page.

Step 2. When the new page appears, click on the **System Components** tab. (This step is not actually necessary since the Networks functional area starts up showing the System Components page; this step is included for completeness.)

Step 3. Click on the label for the desired Access Control Server.

Step 4. When the new page appears, check or uncheck the **Enable SSH command line interface** checkbox.

Note: *For network and maintenance functions, once you have reached the correct page of the Administrative Console you may still need to select the 700wl Series system component you wish to configure. This is done using the System Components List.*

Configuration Functions

The following table shows where to find the proper page in the version 4 Administrative Console for each configuration function in version 3.1.

Function	Path to that Function in the New Administrative Console
Admin Authorization: Set Admin username and password	**Network ⇨ System Components ⇨** *<Access Control Server>*
Admin Authorization: Enable Technical Support Access	**Network ⇨ System Components ⇨** *<Access Control Server or Access Controller>*: **Enable HP ProCurve technical support access**
HTTP Proxy	**Network ⇨ Network Setup⇨** *<Access Controller>* **⇨ HTTP Proxy**
Basic Network Configuration	**Network ⇨ Network Setup⇨** *<Access Control Server or Access Controller>* **⇨ Basic Setup**
Advanced Network Configuration: (Access Control Server)	**Network ⇨ Network Setup⇨** *<Access Control Server>* **⇨ Advanced Setup:**
• DHCP Network for NAT Clients	• **DHCP Network for NAT Clients**
• Port Settings	**Network ⇨ Interfaces ⇨ Speed/Duplex** (for setting connection type)
Advanced Network Configuration: (Access Controller)	**Network ⇨ Network Setup⇨** *<Access Controller>* **⇨ Advanced Setup:**
• Bridging	• **Bridging**
• Client Probes	• **Client Polling**
• Broadcasting	• **Forward IP Broadcasts…**
• Port Settings	**Network ⇨ Interfaces ⇨ Speed/Duplex** (for setting connection type) **Network ⇨ Interfaces ⇨ Subnet** (for setting port subnet address and mask)
Shared Secret Authorization	**Network ⇨ System Components ⇨** *<Access Control Server>* **⇨ Shared Secret**
SNMP	**Network ⇨ SNMP**
Specify Location Information	**Rights ⇨ Connection Profiles⇨ Locations**
Specify Session Logging	**Logs ⇨ Logging Setup**
Time and Date Configuration	**Network ⇨ Date & Time**

System Functions

The following table shows where to find the proper page in the new Administrative Console for each system function in version 3.1.

Function	Path to that Function in the New Administrative Console
Backup and Restore	**Maint ⇨ Backup & Restore**
Distribute Logons	*No longer applicable; now all logons are automatically distributed.*
Shutdown: (Reboot, Shutdown, Reset to Defaults)	**Maint ⇨ Shutdown/Restart**
Update Software	**Maint ⇨ Software Setup**

Views

The following table shows where to find the proper page in the version 4 Administrative Console for each system view function in version 3.1.

Function	Path to that Function in the New Administrative Console
View Active Access Controllers	**Status ⇨ Equipment Status**: Access Controllers tab
View Active Clients	**Status ⇨ Client Status**
View Active Sessions	**Status ⇨ Session Status**
View Log File	**Logs ⇨ Log Files**
View Version Information	**Status ⇨ Equipment Status** or **Maint ⇨ Software Setup**
View License Information	**Status ⇨ License Information**

Wireless Data Privacy Setup

The following table show where to find the proper page in the version 4 Administrative Console for each configuration function in version 3.1.

Function	Path to that Function in the New Administrative Console
IPSec Configuration	**VPN ⇨ Wireless Data Privacy**
IPSec Certificate Configuration	**VPN ⇨ Certificates**
PPTP and L2TP (enable)	**VPN ⇨ Wireless Data Privacy**
SSH (enable)	**VPN ⇨ Wireless Data Privacy**
Tunneling Configuration	**VPN ⇨ IP Address Assignment**

Rights Manager

The following table show where to find the proper page in the version 4 Administrative Console for each configuration function in version 3.1.

Function	Path to that Function in the New Administrative Console
Clients	**Status ⇨ Client Status**
Clients: Setting up Access Points	**Rights ⇨ Identity Profiles ⇨ Network Equipment ⇨ New Equipment** or **Rights ⇨ Identity Profiles ⇨ Network Equipment ⇨** *<access point>*
Configuration: Accounting	**Rights ⇨**
• Services	• **Authentication Policies ⇨ Authentication Services ⇨ New Service ⇨ RADIUS** or *<RADIUS Authentication Service>*: **Enable RADIUS Accounting**
Configuration: Authentication	**Rights ⇨**
• Authentication Services	• **Authentication Policies ⇨ Authentication Services**
• Authentication Realms	• **Authentication Policies**
• Customize Web Pages	• **Logon Customization**
• Encryption/Authentication per Location: Encryption	• **Access Policies ⇨ New Access Policy** or *<Access Policy>* **⇨ Encryption** and **Encryption Protocols**
• Encryption/Authentication per Location: PPTP/L2TP Authentication	• **Access Policies ⇨ New Access Policy** or *<Access Policy>* **⇨ Authentication for PPTP or L2TP**, **MPPE** and **Key Length**
• Monitored Logon: Enable 802.1x per Where	**Authentication Policies ⇨ New Authentication Policy** or *<Authentication Policy>*: select *NT Domain Logons* or *802.1x Logons*.
• Monitored Logon: 802.1x Logon Settings	• **Authentication Policies ⇨ Authentication Services**: click *802.1x Logons* in the table
• External Group Retrieval	• **Authentication Policies ⇨ External Identity Retrieval**
• Retrieve MAC Address Users	• **Identity Profiles ⇨ MAC Address Retrieval**
Configuration: Control Console	Not available in version 4
Configuration: DNS/WINS:	**Rights ⇨**
• DNS Servers	• **Access Policies ⇨ DNS Filters**
• DNS Allow/Redirect Pairs	• **Access Policies ⇨ DNS Filters**
• WINS Servers	• **Access Policies ⇨ WINS Filters**
• WINS Allow/Redirect Pairs	• **Access Policies ⇨ WINS Filters**
Configuration: Automatic HTTP Proxy per Group	**Rights ⇨ Access Policies ⇨ New Access Policy** or *<Access Policy>* **⇨ HTTP Filters**
Configuration: Setup Logging	**Logs ⇨ Logging Setup**
Configuration: Security	**Network ⇨ Network Setup⇨** *<Access Control Server>* **⇨ Advanced Setup**
• Spoofing Detection	• **MAC Address Spoofing Detection**
• SSL Certificate	**Network ⇨ Network Setup⇨** *<Access Control Server>* **⇨ SSL**

Function	Path to that Function in the New Administrative Console
Users	**Rights ⇨ Identity Profiles ⇨ Users**
Groups	**Rights ⇨ Identity Profiles ⇨**
• Group/New Group	• **New Identity Profile** or <*Identity Profile*>
• Allows/New Allow	• **Allowed Traffic Filters** or <*Allowed Traffic name*>
• Redirects/New Redirect	• **Redirected Traffic Filters** or <*Redirected Traffic name*>
Locations	**Rights ⇨ Connection Profiles ⇨**
• Location/New Location	• **New Connection Profile** or <*Connection Profile*>
• Edit/New Where	• **Locations ⇨ New Location** or <*Location*>
New AM/Edit AM	• **Network ⇨ System Components**: Access Controllers configured with Access Control Server IP address and shared secret are automatically detected
• Edit/New When	• **Time Windows ⇨ New Time Window** or <*Time Window*>
Logs	**Logs ⇨ Log Files**
Troubleshooting:	**Rights ⇨ Tools & Options ⇨**
• User Rights Simulator	• **Simulate User Rights**
• Transaction Tracer	• **Trace Transaction**
Rights Import	**Rights ⇨ Tools & Options ⇨ Import/Export Rights**

June 2004

Manual Part Number
5990-8807