# Upgrading Software
# Version 3.1 to Version 4

HP ProCurve
Secure Access
700wl Series

www.hp.com/go/hpprocurve

# HP PROCURVE
# SECURE ACCESS 700WL SERIES

# UPGRADING SOFTWARE VERSION 3.1 TO VERSION 4

**Publication Number**

5990-8808
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 *Upgrading Software Version 3.1 to 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:

- Upgrade your 700wl Series system to version 4
- Migrate your existing system configuration, including access rights, to version 4

## 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 procedural information describing how to upgrade from 700wl Series system version 3.1 to version 4, and how to migrate your rights configuration from version 3.1 to version 4.

***Note:*** *It is strongly recommended that you read the Introduction to Software Version 4 before you begin the upgrade process. The version 4 Rights Manager in particular is quite different from the version 3.1 Rights Manager structure, and should be thoroughly understood before you attempt to migrate the rights configuration.*

# 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. |
| *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 a brief overview of what is new in this release of the 700wl Series system, and describes the upgrade process.

## Chapter 2—“Upgrading your System”

This chapter steps you through the process of upgrading your current 700wl Series system from version 3.1 to version 4. When this process is completed you are able to use and manage the version 4 system, including version 4 features such as bandwidth management.

## Appendix A—“System Upgrade Checklist”

This appendix provides a checklist of the steps required for upgrading your current 700wl Series system to the version 4. Once you have read this guide, use the “System Upgrade Checklist” as a convenient guide to performing all the necessary steps in the correct order.

### Appendix B—"Functionality Changes"

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

- Terminology changes
- Functionality changes
- New functionality

### Appendix C—"Function Map: Version 3.1 to Version 4"

This appendix is a table that shows users experienced with the version 3.1 Administrative Console where to find each function in the version 4 Administrative Console. Functions are grouped in the same way they are in the version 3.1 Administrative Console. Consult this appendix if you need to find where to perform some function you are familiar with in the version 3.1 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 |
|---|---|
| *Introduction to Software Version 4* | For users familiar with older versions of the 700wl Series system it describes what is new and what is different in the current release, and provides an overview of the version 4 Administrative Console<br>Available in PDF format on the technical support pages of the HP ProCurve website 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.<br>This guide is available in both PDF and HTML format from the Help button within the Administrative Console.<br>Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve website at www.hp.com/go/hpprocurve |
| *HP ProCurve Secure Access 700wl Series Installation and Getting Started Guide*<br>*(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.<br>Shipped with each Access Control Server or Integrated Access Manager.<br>Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve website at www.hp.com/go/hpprocurve |
| *HP ProCurve 700wl Series Quick Start Guide*<br>*(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.<br>Shipped with each hardware unit<br>Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve website 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.<br>Available in PDF format on the documentation CD shipped with each hardware unit, and on the technical support pages of the HP ProCurve website 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 website at www.hp.com/go/hpprocurve. |

# 1

# INTRODUCTION

This guide provides step-by-step instructions for upgrading a 700wl Series Version 3.1 configuration to version 4. It assumes that the reader has read the *HP ProCurve Secure Access 700wl Series Introduction to Software version 4*. The topics in this chapter are:



## Migrating to 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 redundant Access Control Servers and Access Control Server failover
- Client-based bandwidth rate limiting
- Enhanced VLAN support

The upgrade and migration process leads you through the steps to upgrade from 700wl Series system version 3.1 and configure the version 4 system so that it provides the same functionality that you had implemented under your 3.1 configuration. This guide does *not* provide instructions for configuring version 4 features such as Access Control Server failover, or bandwidth rate limiting. To learn about and configure the new features available with release 4, you should see the *700wl Series System Management and Configuration Guide* for version 4.

## 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 version 4 Rights model.*

With previous releases of the 700wl Series system software, each new release was backwards-compatible: after the upgrade. The complete system configuration, including the Rights Manager configuration, was preserved and was still functional after the upgrade. 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 version 4 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 version 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.

The software upgrade itself is done through the normal Software Upgrade function accessed through the Administrative Console or the command line interface (CLI).

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.

It is strongly recommended that, if possible, you upgrade an Integrated Access Manager, or an Access Control Server and an Access Controller to version 4 in a lab or test-bed environment, where you can recreate your Rights configuration and verify that the system functions as expected before you upgrade your entire 700wl Series system. If you maintain an Access Control Server or Integrated Access Manager running version 3.1, you can continue to provide network access to clients through the version 3.1 Access Control Server and Access Controllers. Otherwise, because Access Controllers running version 3.1 cannot communicate with an Access Control Server running version 4, no new clients will be able to connect to the network, existing clients will not be able to roam, and other disruptions in client access may occur.

Once you have your version 4 system functioning correctly, you can upgrade any additional Access Controllers to version 4, and by simply reconfiguring their Access Control Server IP address and the shared secret to reference your version 4 Access Control Server, those Access Controllers will automatically become part of the functioning version 4 system.

As with previous upgrades, the upgrade preserves the network configuration settings. However, ***much of the 3.1 Rights Manager configuration is not preserved!*** The version 4 Rights Model is simpler to configure, and in many cases much of the version 3.1 configuration may no longer be relevant. However, immediately upon upgrade, only a default rights configuration will be in effect.

Because the migration process requires that you recreate your Rights functionality under the version 4 Rights model, it is recommended that you export your version 3.1 Rights configuration before you upgrade your Access Control Server or Integrated Access Manager. The migration instructions have you export your Rights to an external file before you upgrade to version 4. Once you upgrade, your version 3.1 rights configuration is no longer accessible.

The migration instructions later in this Guide lead you through the process of creating Identity Profiles, Connection Profiles, Access Policies and Authentication Policies that map the functionality of your 3.1 groups, locations and Authentication Realms.

## What Is Automatically Transferred

The following parts of the 700wl Series system data are migrated automatically to version 4 when the system software is upgraded:

- Wheres—These are transferred into *locations*
- Whens—These are transferred into *time windows*
- Allows (both system and user-defined)
- Redirects (both system and user-defined)
- Authentication services
- Authentication Realms become Authentication Policies
- The built-in user database, with all the user data (clients of type Access Point appear in the version 4 Network Equipment category)

***Note:*** *In the 3.1 software, the names for 700wl Series system elements (Wheres, Whens, Allows and Redirects, Users etc.) were effectively unlimited in length (the limit was 65,535 characters). In the version 4 software, the limit for most names is 32 characters. If you use names that contain more than 32 characters, the item will be migrated but the name will be truncated.*

## What Must Be Manually Transferred

Since the way rights are associated with users has changed, the version 3.1 groups, locations, Authentication Realms, and HTTP Proxy Filter settings from version 3.1 are not migrated automatically to version 4 when the system software is upgraded. You must create new Identity Profiles, Connection Profiles, and Access Policies that map the functionality of your 3.1 groups and locations:

- What were Groups (of users) ⇨ new Identity Profiles
- What were Groups (of rights) ⇨ new Access Policies
- What were Locations ⇨ new Connection Profiles

Once these are set up you combine them in the version 4 Rights Assignment table, which is the mechanism the version 4 700wl Series system software uses to determine rights for clients.

# 2

# UPGRADING YOUR SYSTEM

This chapter presents the steps required to upgrade and migrate your system from 700wl Series system software version 3.1 to version 4. The topics covered include:



## Overview of the Migration Process

When you upgrade from version 3.1 to 4, most of your 3.1 configurations are preserved. However, some of your rights configuration—specifically groups and locations—will not be preserved. Part of the migration process is to recreate, in the new version 4 system, the access control functionality embodied in your version 3.1 groups and locations. Therefore, it is important that you read and understand Chapter 3, "The New Rights Manager", before you upgrade to version 4.

***Note:*** *This Guide leads you through upgrading and migrating your 3.1 system so that it performs with equivalent functionality as it had before you migrated. It does not cover configuring version 4 features such as Access Control Server Failover. Version 4 features are explained in the HP ProCurve Secure Access 700wl Series Migration and Configuration Guide.*

The basic steps to upgrade and migrate from version 3.1 to version 4 are the following:

**Step 1.** Make sure that your system is configured for distributed logons (Access Control Server or Integrated Access Manager only).

> ***Note:*** *Centralized Logon is no longer supported as of version 4. Distributed logon was the default in version 3.1, but systems that had been configured to use centralized logon were still supported. This is no longer true in version 4. Systems that use centralized logon are automatically set to use distributed logon after the upgrade. It is recommended that you configure your 3.1 system for distributed logon and verify that your system continues to function as you expect* ***before*** *you upgrade to version 4.*

**Step 2.** Back up your system (do this for each 700wl Series system component: Access Control Server, Integrated Access Manager, and all Access Controllers). For an Integrated Access Manager you back up the Access Control Server module and the Access Controller module as a unit.

**Step 3.** Export the rights (Access Control Server or Integrated Access Manager only). This provides a record of the rights configuration as it existed in 3.1. You need this to aid in recreating your rights configuration in the version 4 rights model.

**Step 4.** Upgrade the software on all components (Access Control Server or Integrated Access Manager, and all Access Controllers).

When upgrading your components we recommend you upgrade the Access Control Server first, then upgrade the Access Controllers.

***Caution:*** *Before you upgrade an Access Controller, you must log off all clients connected through that Access Controller. If you do not, the upgrade may fail.*

For Access Controllers, if you have not changed the shared secret on the Access Control Server, this completes the migration. The remaining steps to accomplish the migration are performed on the Access Control Server or Integrated Access Manager.

***Note:*** *On an Access Controller, if you upgraded through the version 3.x Administrative Console and specify an immediate reboot, when the reboot completes you will be presented with the version 4 Administrator login page. However, if you log on, your only option (besides logging out) will be a link to the version 4 Access Control Server Administrative Console. In version 4 you can no longer access an Administrative Console on an Access Controller.*

**Step 5.** Logon to the Administrative Console of your Access Control Server or Integrated Access Manager, and configure version 4 rights components by doing the following:

**a.** Edit the built-in Default Authentication Policy to match the authentication services you use

**a.** Create Identity Profiles based on your 3.1 groups

**b.** Recreate any customized logon pages

**c.** Create Connection Profiles based on your 3.1 locations

**d.** Edit the built-in Unauthenticated Access Policy and create new Access Policies based on options from your 3.1 group and location settings, encryption settings, and HTTP proxy filter settings.

This configuration only needs to be done on your Access Control Server or Integrated Access Manager; the configuration is propagated automatically to all the Access Controllers.

**Step 6.** Build a Rights Assignment Table using the elements created in Step 5. (Building the Rights Assignment Table only needs to be done on your Access Control Server or Integrated Access Manager; the information is propagated automatically to all the Access Controllers).

To upgrade your Access Control Server or Integrated Access Manager, you must perform all the steps from Step 1 to Step 6. This restores functionality to match that of the system under 3.1.

To upgrade an Access Controller, you only perform Step 2 and Step 4 (backing up your system and updating the software). You must also ensure that no clients are logged on during the time you are doing the upgrade (you can **Log off all clients** from the Rights Manager Clients page).

## Making Configuration Changes after the Upgrade

Once you have migrated your system to version 4, all further configuration and management tasks should be performed from the centralized Administrative Console on the primary Access Control Server. Even configuration of Access Controller features—such providing a name for the Access Controller,

configuring port speed settings, or viewing client status—are performed from the centralized Administrative Console.

***Caution:*** *It is still possible to access an Access Controller through its Command Line Interface.* ***Do not make configuration changes through the Access Controller CLI****. Because the Access Control Server maintains knowledge of each Access Controller configuration, changes you make directly on the Access Controller may be overwritten by the Access Control Server when it next propagates its version of the Access Controller settings to the Access Controller.*

After the upgrade, you may wish to implement some of the new features found in version 4, such as adding bandwidth management settings, organizing your Access Controllers into folders, or adding a second Access Control Server for redundancy. These new features are described in Chapter 1, and are discussed in detail in the *700wl Series System Configuration and Management Guide*.

# Prepare for the Upgrade

## Step 1: Configure The System for Distributed Logons

Centralized Logon is no longer supported. Systems that use Centralized Logon are automatically set to use Distributed Logon after the upgrade. It is strongly recommended that you configure your 3.1 system for Distributed Logon and verify that your system continues to function as you expect *before* you upgrade to version 4. This step is only done on the Access Control Server or Integrated Access Manager.

## Step 2: Back Up the System

Once you have installed version 4, you will not be able to downgrade to 3.1 without causing a factory reset, which sets your configuration back to its default settings. If for any reason you need to return to your previous software version, you need a saved backup in order to restore your settings. If you have an Integrated Access Manager, this step is done once on the Integrated Access Manager. If you are running an Access Control Server, you need to back up the Access Control Server and back up all the Access Controllers.

To back up your system:

**Step 1.** On the Main Menu, click the **Backup and Restore** link. This takes you to the Backup and Restore page.

**Step 2.** Click **Create Backup**. This initiates the backup process.

> ***Note:*** *This creates a backup image in the 700wl Series system component, but does not save it to a file. You must save the backup as a file on your local system to have it available to be restored, should the need arise.*

**Step 3.** When the backup is complete, click **Save Backup**. You are prompted for a location and a filename for the backup file. Remember this location and filename, as you may need the file later.

## Step 3: Export Rights

Once you upgrade to 4, the locations and groups in your version 3.1 rights configuration are lost. You need to recreate them as Connection Profiles and Identity Profiles, based on your 3.1 configuration. To assist with recreating your rights configuration, export the rights file before you upgrade to version 4. The exported rights file provides a record of the rights configuration that was in place under your version 3.1 software. This step is only done on the Access Control Server or Integrated Access Manager.

The **Export Rights** command creates an XML file that defines your entire rights configuration. The file can be quite long, especially if you have a large number of users in your built-in database. Of significance for the migration process is that it specifies the attributes of your groups, locations, HTTP proxy filters, and Customized Logon pages, which you must recreate in the version 4. If you have a large number of groups, locations, proxy filters *etc.* it may be very difficult to remember all the settings that pertain to each one without access to the exported rights file.

To export your current rights:

**Step 1.** On the Main Menu, click the **Rights Manager** button. This takes you to the Rights Manager page.

**Step 2.** Click **Rights Import** to bring up the Rights Manager Import/Export page.

**Step 3.** Under **Export Rights** click the **Create** button to create a new export image.

> ***Note:*** *This creates an export image in the 700wl Series system Access Control Server or Integrated Access Manager, but does not save it to a file. You must save the export file on your local system to have it available.*

**Step 4.** When the rights file has been created, click **Download**. You are prompted for a location and a filename for the export file. Remember this location and filename as you need the file later.

# Upgrade the Software

## Step 4: Update the System Components

Once you have backed up your system, exported the rights configuration, and noted the Encryption/Authentication per location information, you can proceed to upgrade your software. You do this through the **Update Software** page.

If you have an Integrated Access Manager, this step is done once on the Integrated Access Manager. If you are running an Access Control Server, you need to upgrade the Access Control Server and upgrade all the Access Controllers.

A new key is required to upgrade to version 4. The key that was valid for your previous version of the software does not work for version 4. To obtain the new key, contact HP ProCurve technical support.

***Note:*** *If this upgrade is for an Access Controller, the process is complete. The remaining steps apply only to the Access Control Server or Integrated Access Manager. You may log off from the Access Controller Administrative Console. All additional Access Controller configuration should be done from the central Administrative Console on the primary Access Control Server.*

## Step 5: Verify System Settings

When you have completed the system software update for all 700wl Series system components, and the system has rebooted, check to see that your previous settings have been preserved. The following settings are preserved after the upgrade. (This list does not include the rights settings that are preserved; for those see "Step 6: Configure the Version 4 Rights Components" on page 2-6.)

To verify the system settings, logon to the Administrative Console on the Access Control Server and verify the following attributes have the correct values. Refer to Chapter 2, "The New Administrative Console" for guidance on where to find these settings in the version 4 Administrative Console.

### Configuration

- Administrator authorization: username and password, and enable SSH technical support access
- HTTP Proxy settings
- The list of active Access Controllers
- Network configuration settings: Hostname, Domain Name. Obtain IP Address via DHCP setting, system IP address, netmask, default router, primary and secondary DNS/WINS settings
- Advanced network configuration settings: bridging, client probes, DHCP network for NAT clients settings, broadcasting, and port settings
- Shared secret
- SNMP settings
- Session logging settings
- Time and date settings

### Wireless Data Privacy

- IPSec configuration
- IPSec certificates
- Tunneling configuration settings

***Note:*** *In the 3.1 software, the names for 700wl Series system elements (Wheres, Whens, Allows and Redirects, Users etc.) were effectively unlimited in length (the limit was 65,535 characters). In the version 4 software, the limit for most names is 32 characters. If you use names that contain more than 32 characters, the item will be migrated but the name will be truncated. You should check to make sure that all your data was transferred correctly.*

# Recreate the Rights Configuration

At this point you have completed the upgrade of the 700wl Series system software to version 4. You now need to recreate the authentication policies and access rights for system users. This is done in the following two steps. For a complete explanation of how access rights and authentication works in the version 4 system, see chapters 4 and 5 of the *700wl Series system Management and Configuration Guide.*

## Step 6: Configure the Version 4 Rights Components

On an Access Control Server or Integrated Access Manager, not all the information kept in the 3.1 Rights Manager can be preserved after the upgrade. You must recreate some of your authentication and access rights configuration.

The following information ***is preserved*** after the upgrade to version 4:

- Authentication services, including the 802.1x RADIUS server configuration
- Authentication Realms (these are transferred into Authentication Policies)
- Allows and Redirects
- Wheres (these are transferred into locations)
- Whens (these are transferred into time windows)
- The built-in database of clients (both normal users and MAC addresses)

Using these elements, you create:

- Authentication Policies
- Connection Profiles
- Identity Profiles
- Access Policies

You then use these to create a set of entries in the Rights Assignment Table, which specifies what access rights are granted to clients and under what conditions.

***Important:*** *The following instructions assume you have read Chapter 3, "The New Rights Manager", in the Introduction to Software Version 4, or have read the appropriate chapters in the HP ProCurve Secure Access 700wl Series Management and Configuration Guide.*

### Configure Authentication Policies

In the 700wl Series system software version 4, Authentication Policies replaces the Authentication Realms found in version 3.1. Like an Authentication Realm, an Authentication Policy is an ordered set of Authentication Services.

Authentication Realms are transferred into Authentication Policies in version 4. Additionally, version 4 comes with a default Authentication Policy, called "System Authentication Policy". Like the Default Realm in 3.1, it includes only the built-in authentication service. The "Default Authentication Realm" in your 3.1 system is transferred into a separate Authentication Policy. To use the version 3.1 default policy transferred from your 3.1 system as the new default, take the following steps:

**Step 1.** Click the Rights icon in the Navigation bar, then click the **Authentication Policies** tab. The Authentication Policies page appears.

**Step 2.** Delete the Default Authentication Policy by clicking on the trashcan icon on the same row as the *Default Authentication Policy*.

**Step 3.** Click the name of your default policy, (e.g., "Default Authentication Realm"*)* in the Authentication Policy column. This displays the Edit Authentication Policy page.

**Step 4.** Put a check in the checkbox next to **Make this the default authentication policy**.

**Step 5.** Optionally, you can change the name of the policy as well (for instance, changing "Default Authentication Realm" to "System Authentication Policy").

**Step 6.** Click **Save.**

### Authentication Policies for NT Domain Logon or 802.1x Logon

In Release 3.1, Monitored Logons (NT Domain Logon and 802.1x Logon) were specified for each Where, through the **Enable 802.1x/NT Domain Logon per Where** page of the Rights Manager.

In release 4, these two authentication mechanisms are handled just like the other authentication service types, and are enabled by including them in an Authentication Policy, and then associating that Authentication Policy with a Connection Profile. NT Domain Logon and/or 802.1x Logon always take precedence (they are always ordered ahead of other services) so any other service is used only if the initial monitored logon fails.

To enable NT Domain Logons or 802.1x Logons:

**Step 1.** Create an Authentication Policy that uses one or both of these authentication services.

If these two are always used together, you can include them in the same Authentication Policy. If they might be used separately for different locations, create a separate Authentication Policy for each one.

You can combine NT Domain Logon and 802.1x Logon with other authentication services in the same Authentication Policy, if you want to specify an alternate authentication method in case the NT Domain or 802.1x logon fails.

**Step 2.** To configure the RADIUS server for 802.1x Logons, edit the 802.1x Logons Authentication Service by clicking its name or clicking the pencil icon at the end of its row.

If you used 802.1x Logons in version 3.1, the RADIUS server should already be configured correctly.

**Step 3.** Associate this Authentication Policy with each Connection Profile that represents the locations where this type of authentication should be used. This is discussed further in the section on Connection Profiles below.

***Note:*** *As was true for 3.1, if you are going to use NT Domain logon to define the rights for users who are authenticated in that manner, the name of the Identity Profile must match the name of the NT Domain in which these users are members.*

## Create an Identity Profile for Each Former Group

All the users and MAC addresses in the built-in database are transferred as part of the system upgrade. You need to associate each user or MAC address with one or more Identity Profiles. For each group of clients, you create an Identity Profile and add users or MAC addresses, or both, to that profile:

**Step 1.** Click the Rights icon in the Navigation bar, then click the **Identity Profiles** tab. The Identity Profiles page appears.

**Step 2.** Click **New Identity Profile…**; this brings up the **New Identity Profile** page.

**Step 3.** Enter the name of the Identity Profile (this can be the same as the version 3.1 group name) in the **Name** field.

**Step 4.** Enter a check in the checkbox of each user or MAC address that is to be part of this Identity Profile.

**Step 5.** If the Identity Profile is to contain network equipment (access points), click the **Network Equipment** sub-tab to see a list of the network equipment and enter a check in the checkbox of each piece of network equipment to be included in this Identity Profile.

**Step 6.** Click **Save**.

***Note:*** *Information about the groups of which a user was a member is given in the rights file you exported. It is found in the Users section for each user, and is tagged as <user_groups>.*

## Recreate Any Custom Logon Pages

Recreate any custom logon pages you had in your 3.1 system. To do this:

**Step 1.** Click the Rights icon in the Navigation bar, then click the click the **Login Customization** tab. The **Login Customization** page appears.

**Step 2.** Click **New Login Customization…**; this brings up the **New Login Customization** page.

**Step 3.** Enter a name for this logon page in the **Name** field at the top of the page. If you wish this to be the default logon page, place a check in the checkbox next to **Make this the preferred login customization**.

**Step 4.** If you wish to add a company or organization logo, you may upload either a large logo or a small one. To do this click the **Browse…** button next to the **Logo** and **Small Logo** entry fields. You can then specify the graphics files on your local system that contain the logos.

If you want the logos to act as graphical links to a URL (for instance the home page for your company or organization), enter the desired URL (including the "http://" prefix) in the **Logo URL** field.

**Step 5.** Enter the text you wish to show in the logon page in the **Logon Page Text** field. You may enter HTML formatting commands in with the text.

***Caution:*** *If you add HTML formatting within your text make certain to close any tags you may open, and match up all quotation marks. Failure to do so may create a malformed logon page.*

**Step 6.** Select who is allowed to logon using this page, Guests, Registered Users, or both. Allowing Guests to use the logon page means that a client can logon without authentication as a guest. They receive whatever access permissions are allowed to guests.

**Step 7.** Use the checkboxes to specify the following options:

- **Allow users to specify authentication service**—Put a check in this checkbox if you want to allow users to select the authentication service (from those allowed in the relevant Authentication Policy) to use for their authentication.

**Require guests to register before logging on**—Put a check in this checkbox if you want to require guests to provide registration information before they can logon.

- **Display logoff window after logging on**—Put a check in this checkbox if you want a small logoff page open in a new window as soon as the user successfully logs on. The user can go to this page to logoff. (This requires that the user's browser supports Javascript).

**Step 8.** If you want to change the text that appears on the Stop page, or the Stop page graphic (the Stop sign), add the desired new Stop page graphic and text in the Stop Page section at the bottom of the page.

**Step 9.** Click **Save**.

If you wish to use a custom template for the Logon, Logoff, Guest Registration, or Stop page, click the Custom Templates sub-tab and enter the templates and template images you wish to use. Consult the on-line help or the *Configuration Guide* for more information. For a complete explanation of how to create custom logon pages, see "Logon Customization" in Chapter 5 of the *700wl Series System Management and Configuration Guide.*

## Create a Connection Profile for each 3.1 Location

You use the information from the version 3.1 locations to create new Connection Profiles. A Connection Profile consists of a list of locations (formerly known as *wheres*), time windows (formerly known as *whens*), an Authentication Policy, and additional settings.

To create a new Connection Profile based on an version 3.1 location:

**Step 1.** Click the Rights icon in the Navigation bar, then click the **Connection Profiles** tab. The Connection Profiles page appears.

**Step 2.** Click **New Connection Profile…**; this brings up the **New Connection Profile** page.

**Step 3.** On the **Settings** tab enter the desired settings:

**a.** Enter the name you wish to give to this Connection Profile in the **Name** field (this can be the same as the name of the version 3.1 location).

**b.** Select the desired logon page to use from the Logon page drop down field. This contains a list of the custom logon pages you just recreated.

**c.** Select the desired Authentication Policy to use from the Authentication Policy drop down, based on the Authentication Realm used by the version 3.1 location you are recreating.

***Note:*** *Information about which Authentication Realm was used by a location is given in the rights file you exported. It is found in the locations section, and is tagged as <realm> for each location.*

**d.** Enter the VLAN identifier setting to use.

***Note:*** *VLAN tag identification for Connection Profiles in version 4 works quite differently than it did for locations in the previous versions: In 3.1, a VLAN tag was added to all packets entering the system through a location. In version 4 the VLAN tag in the arriving packet is used in determining whether the client matches a Connection Profile or not. Connection Profiles match not only on Identity Profile, location, and time window, but also on VLAN tag. For a fuller explanation, see "Connection Profiles" in Chapter 4 of the "700wl Series system Management and Configuration Guide."*

**e.** Enter the maximum number of concurrent users logons in the **Maximum User Logons** field. If you wish to have the maximum number of concurrent users be unlimited, leave this field blank.

**f.** Click the **Locations** sub-tab and put a check next to all the locations (which used to be *Wheres*) to which this Connection Profile is to apply.

**g.** Click the **Time Windows** sub-tab and put a check next to all the time windows (which used to be *Whens*) to which this Connection Profile is to apply.

**h.** Click **Save.**

***Note:*** *The version 3.1 location Information is given in the rights file you exported. It is found in the locations section for each location, and is tagged as <location_date name>, <vlan_id>, <max_users>, <loc_wheres>, and <whens>, respectively. If a tag is missing that means no such setting was made. For instance a missing <vlan_id> tag means that no VLAN ID was specified.*

Repeat this process for each new Connection Profile you wish to create.

***Note:*** *If you wish to have access rights change based on the Identity Profile, but still allow login via the same location, you create multiple Identity Profiles and different Access Policies. Users in the different Identity Profiles can logon from the same location and in the same time window, but are assigned different Access Policies based on their Identity Profile.*

## Create Access Policies

The access information that was contained in the version 3.1 groups is now contained in Access Policies. To set up the access allowed in your 3.1 system, you need to create a set of Access Policies.

There are three built-in Access Policies, the *Unauthenticated* Access Policy, the *Authenticated* Access Policy, and the *Guest* Access Policy. These Access Policies correspond to the *Logon, (Implicit) Uses,* and *Guest* groups in version 3.1. You need to review the settings for these policies and modify them as needed so that they conform to the access policies of your version 3.1 system:

- The *Unauthenticated* Access Policy should match the authentication and access provided your version 3.1 *Logon* group. In other words, the *Unauthenticated* Access Policy should use the same addressing, allows, redirects, HTTP filters, and timeout settings as your version 3.1 *Logon* group.
- The *Authenticated* Access Policy should match the authentication and access provided your version 3.1 *(Implicit) User* group; the *Authenticated* Access Policy should use the same addressing, authentication methods, allows, redirects, HTTP filters, and timeout settings as your version 3.1 *User* group.
- The *Guest* Access Policy should match the authentication and access provided your version 3.1 *Guest* group; the *Guest* Access Policy should use the same addressing, authentication methods, allows, redirects, HTTP filters, and timeout settings as your version 3.1 *Guest* group.

To edit the *Default Authentication Policy*, or to create a new Access Policy based on an version 3.1 group:

**Step 1.** Click the Rights icon in the Navigation bar, then click the **Access Policies** tab. The **Access Policies** page appears.

**Step 2.** Click **New Access Policy…**; this brings up the **New Access Policy** page.

**Step 3.** Enter the desired name for this Access Policy in the **Name** field at the top of the page (this can be the same as the name of the version 3.1 group).

**Step 4.** Click on the **Settings** tab and enter the desired settings:

**a.** Select the desired NAT setting, "Always", "When Necessary" or "Never", from the **Network Address Translation** drop down.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <nat> (this tag indicates whether NAT is required) and <never_nat> (this tag indicates whether NAT is allowed).A setting of <nat>1</nat> means NAT is required ("Always"); A setting of <never_nat>0</never_nat> and <nat>0</nat> means NAT is allowed when necessary, but not required ("When Necessary"), and a setting of <never_nat>1</never_nat> means never use NAT ("Never").*

**b.** Select the desired IP addressing scheme, either "Allow Static IDP" or "Require DHCP", from the **IP Addressing** drop down.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group. There is a <static_ip>1</static_ip> tag if the version 3.1 group allowed static IP addressing; if this is missing then DHCP was required.*

**c.** Enter the desired maximum number of concurrent logons per user in the **Maximum Number of Concurrent Logons per User** field. If you wish the maximum number to be unlimited leave this field blank.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <max_logons>.*

**d.** Select the encryption setting from the **Encryption** pulldown.

***Note:*** *This information is given in the rights file you exported. It is found in the locations section, and is tagged as <enc_enable> and <enc_req>. A setting of <enc_req>1</enc_req> means encryption is required; A setting of <enc_enable>1</enc_enable> and <enc_req>0</enc_req> means encryption is allowed, but not required.*

***Note:*** *In version 3.1 encryption was by location. You need to find the relevant version 3.1 locations that apply to this Access Policy. If two or more location are applicable, and their settings differ, you create multiple Access Policies and match them to the different Connection Profiles corresponding to the version 3.1 locations.*

**e.** Put a check in the checkbox next to each of the desired encryption protocols to use with this Access Policy.

***Note:*** *This information is given in the rights file you exported. It is found in the locations section, with a separate tag for each type of encryption that is enabled: <pptp_enable>, <ipsec_enable>, <l2tp_enable>, <ssh_enable>. If a tag is missing that type of encryption is not enabled.*

**f.** If this access method uses PPTP, select the desired MPPE setting from the **MPPE** drop down.

***Note:*** *This information is given in the rights file you exported. It is found in the locations section, and is tagged <mppe_stateful>.*

**g.** If this access method uses PPTP, select the desired encryption key length setting from the **Key Length** pulldown.

***Note:*** *This information is given in the rights file you exported. It is found in the locations section, and is tagged <key_len>.*

**h.** Select the desired authentication method by clicking the appropriate radio button, either **Use Associated Authentication Policy** or **Use shared secret**. If you select **Use shared secret**, enter the shared secret value in the **Shared Secret** text field and again in the **Confirm** text field to confirm it.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, indicated by a <realm> tag, if an authentication method is used, or a <secret> tag, if a shared secret is used.*

***Note:*** *If a shared secret is used, the rights file you exported shows the secret as an encrypted string for security purposes.*

**i.** Select the desired MSCHAP setting from the **MSCHAP** drop-down.

***Note:*** *This information is given in the rights file you exported. It is found in the locations section, and is tagged as <mschap_1> and <mschap_2>.*

**j.** Enter a check mark in the checkbox for **Allow PAP for L2TP** pulldown, if desired.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <l2tp_pap>.*

**Step 5.** Click on the **Allowed Traffic** tab and put a check in the checkbox for all the Allow filters that apply to this Access Policy.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <allows>.*

**Step 6.** Click on the **Redirected Traffic** tab and put a check in the checkbox for all the Redirected Traffic filters that apply to this Access Policy.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <redirects>*

**Step 7.** Click on the **HTTP Proxy** tab and enter the desired settings:

**a.** Select the desired Automatic HTTP Proxy setting from the **Automatic HTTP Proxy** pulldown.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group. The setting should be* **Enabled** *if there is a <proxy_enable>1</proxy_enable> entry and* **Disabled** *if there is not.*

**b.** Enter the monitored ports in the **Monitored Ports** text field. If there is more than one port separate the port numbers with commas.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <proxy_ports>.*

**c.** If a tcpdump string is used, enter a check in the **Use tcpdump string** checkbox and enter the string in the **Monitored Ports** text field.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <proxy_regex_enabled> and <proxy_regex>.*

**d.** Add all the HTTP proxy filters needed for this access policy.

***Note:*** *This information is given in the rights file you exported. It is found in the Proxy_Filter_Rules section. Proxies for the version 3.1 group are indicated by their <group_name> tag. For instance, proxy filters that contain <group_name>Guest</group_name> belong to the Guest group.*

To create a new proxy filter, click **New Filter…**; this brings up the **New Filter: HTTP Proxy** page.

Enter the following information and click **Save**.

**Table 2-1. HTTP Proxy Filter Settings**

| Field | Meaning and Information to Enter |
|---|---|
| **Name** | Enter a descriptive name for this filter. Filters from 3.1 systems did not have a name, so there is nothing to transfer from the version 3.1 system into this field. |
| **Description** | (Optional) Enter a short description of this filter. Filters from 3.1 systems did not have descriptions, so there is nothing to transfer from the version 3.1 system into this field. |
| **Proxy Filter** | Enter the type of proxy filter:<br>• Allow IP address(1)/Deny IP address(6)<br>• Allow FQDN(2)/Deny FQDN (7) (fully qualified domain name)<br>• Allow Host(3)/Deny Host(8) (host name)<br>• Allow Net(4)/Deny Net(9) (destination network address—IP address and subnet mask)<br>• Allow Reg(5)/Deny Reg(10) (regular expression that evaluates to a destination address or address range)<br>• Allow All (200)/Deny All (100)<br>***Note:*** *This information is given in the rights file you exported. It is found in the Proxy_Filter_Rules section. Proxies for the version 3.1 group are indicated by their <group_name> tag. For each proxy filter there is a <rule_type> tag. Each filter type corresponds to a tag number; the appropriate tag for each filter type is given above in parentheses. For instance, the proxy filter type of "Allow IP" corresponds to rule_type 1.* |

**Table 2-1. HTTP Proxy Filter Settings (Continued)**

| Field | Meaning and Information to Enter |
|---|---|
| **Details** | Enter any parameters needed to complete the specification of the filter:<br>• Allow/Deny IP address—Enter the destination IP address<br>• Allow/DenyFQND—Enter the destination fully qualified domain name<br>• Allow/Deny Host—Enter the destination host name<br>• Allow/Deny Net—Enter the destination network address (IP address and subnet mask)<br>• Allow/Deny Reg—Enter a regular expression that evaluates to a destination address or range<br>• Allow/Deny All—No details are necessary |
| **Verify via DNS** | Enter a check in this checkbox to specify that the 700wl Series system should verify the destination name or address via DNS before forwarding it to the proxy server. (This is a relatively costly operation in terms of time; use sparingly. |

**e.** When you have completed entering all the HTTP proxy filters, return to the HTTP Proxy sub-tab for the Access Policy. Put a check in the checkbox next to all the filters that apply to this HTTP proxy (i.e., all the filters you have just created).

**f.** Order the filters appropriately. Use the up and down arrow buttons ( ) to move each proxy filter to the appropriate location. The first proxy filter to run should be at the top, and the last filter should be at the bottom.

***Note:*** *This information is given in the rights file you exported. It is found in the Proxy_Filter_Rules section. Proxies for the version 3.1 group are indicated by their <group_name> tag. For each proxy filter there is a <rule_number> tag, indicating the relative location of this rule. The last rule has a rule number of 999.*

**Step 8.** Click on the **Timeout** tab and enter the desired settings:

**a.** Enter the desired Linger timeout setting in the **Linger Timeout** field.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <linger>.*

**b.** If the version 3.1 group had an expiration type of *relative expire,* click on the radio button next to **Force users to reauthenticate after a specified amount of time** and enter the relative expiration value in the **Reauthenticate after** field. You can enter a value in minutes, hours, or days.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <expire>. The value given is in seconds.*

**c.** If the version 3.1 group had an expiration type of *fixed expire time,* click on the radio button next to **Force users to reauthenticate at a fixed time of day** and enter the desired time of day in the **Reauthenticate after** field.

***Note:*** *This information is given in the rights file you exported. It is found in the groups section for the version 3.1 group, and is tagged as <fixed_expire>. The value given is in HH:MM:SS format, using a 24-hour clock.*

**d.** If the version 3.1 group never forced users to reauthenticate (if steps **b** and **c** above do not apply), click on the radio button next to **Never force users to reauthenticate**.

**Step 9.** Click **Save**.

Repeat this process for each new Access Policy you wish to create.

## Step 7: Add Rows to the Rights Assignment Table

Once you have created all the Identity Profiles, Connection Profiles, and Access Policies, you combine these in the Rights Assignment Table. This table consists of an ordered set of rows. Each row matches an Identity Profile and a Connection Profile pair to an Access Policy. In other words, based on who the user is (the Identity Profile) plus where, when, and how they are connecting to the system (the Connection Profile) they are assigned a set of access rights (the Access Policy).

If you have maintained the naming convention from the version 3.1 system, creating these rows should be straightforward. For instance, the information contained in the version 3.1 groups was split into Identity Profiles and Access Policies; to create the proper row in the Rights Assignment Table, you match the names of the Identity Profiles and the Access Policies.

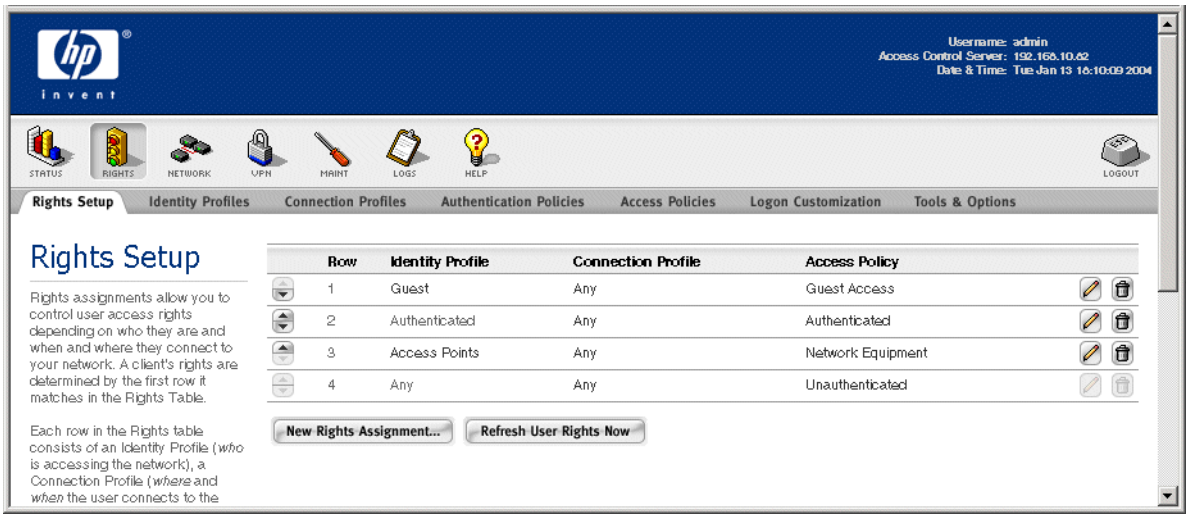
The 700wl Series system looks for a matching row starting at the top of the table, and stops at the first match. Thus, the order of rows in the table is important. Note that the default, catch-all row for any Identity Profile and any Connection Profile is fixed as the last row in the table. This row guarantees that all users always match at least one row in the table, and that this catch-all rule is only used if no other rule applies. Place the more restrictive rules at the top of the table and the more general rules below them.

To understand how the Rights Assignment Table is used by the 700wl Series system, carefully review the examples of how the Rights Assignment Table works given in “Using the Rights Assignment Table: Examples” on page 3-15, in Chapter 3, “The New Rights Manager”.

Initially, the Rights Assignment Table has only three rows (see Figure 2-1.):

- A catch-all assignment rule that matches any Identity Profile and any Connection Profile with an *Unauthenticated* Access Policy. (The Unauthenticated Access Policy is the equivalent of the access settings for the version 3.1 *Logon* group.)
- An assignment policy that matches anyone in the Guest Identity Profile and any Connection Profile with a *Guest* Access Policy. (The Guest Access Policy is the equivalent of the access settings for the version 3.1 *Guest* group.)
- An assignment policy that matches anyone in the Authenticated Identity Profile and any Connection Profile with an *Authenticated* Access Policy. (The Authenticated Access Policy is the equivalent of the access settings for the version 3.1 *Users* group.)

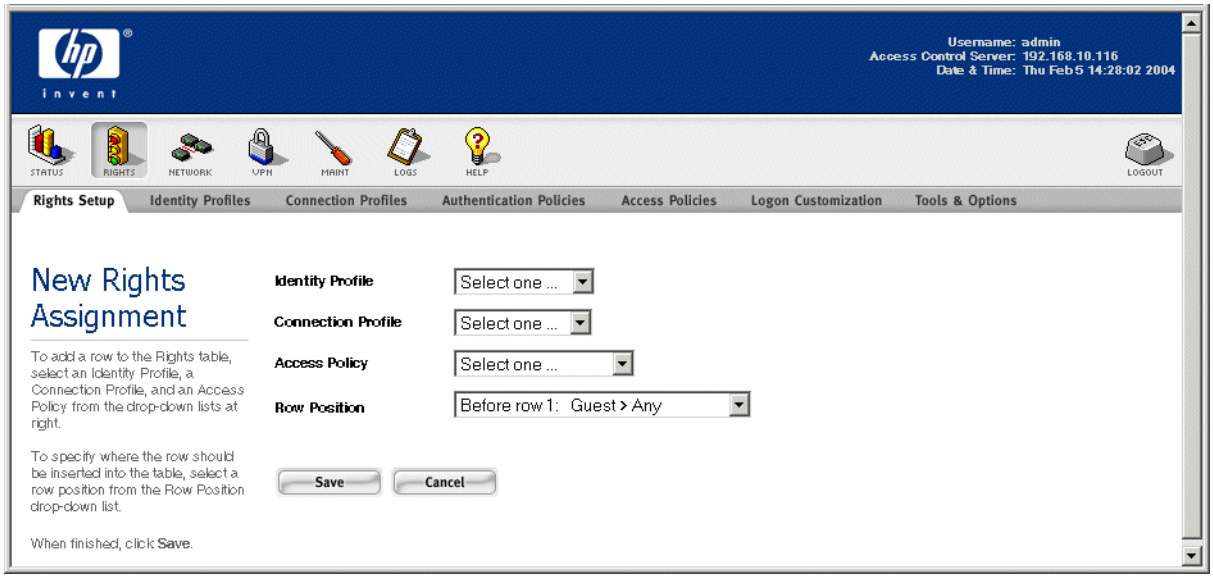
**Figure 2-1. Rights Assignment Table: Initial State**




## Adding a Rights Assignment

To add a new row to the Rights Assignment Table, click the **New Rights Assignment...** button at the bottom of the table. The New Rights Assignment page appears, as shown in Figure 2-2.

**Figure 2-2. New Rights Assignment Table**




**Step 1.** Select the desired Identity Profile from the **Identity Profile** drop-down list.

**Step 2.** Select the Connection Profile from the Connection Profile drop-down list.

**Step 3.** Select the appropriate Access Policy from the Access Policy drop-down list.

**Step 4.** Specify the location of the row using the Row Position drop-down list.

**Step 5.** Click **Save**.

***Note:*** *If the position of the row needs to be change you can do this using to up & down row position buttons to the left of the row in the Rights Assignment Table.*

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

## Migrating Rights: An Example

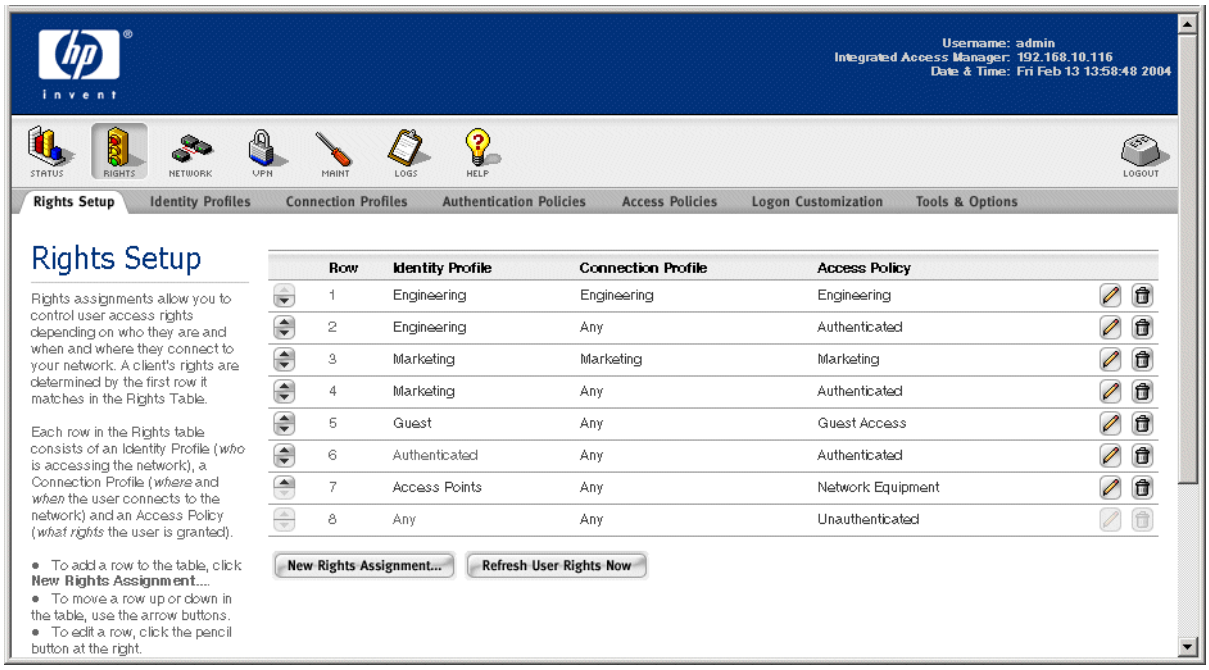
To make the migration of Groups and Locations to Identity Profiles, Connection Profiles, and Access Policies clearer, consider the following 3.1 system to be upgraded to version 4.

| Version 3.1 Location ⇨ | Version 4 Connection Profile |
|---|---|
| Engineering | Engineering |
| Marketing | Marketing |
| Everywhere Else | Any |

| Version 3.1 Group ⇨ | Version 4 Identity Profile | version 4 Access Policy |
|---|---|---|
| Engineers | Engineering | Engineering |
| Marketing | Marketing | Marketing |
| Guest | Guest | Guest |
| Logon | Any | Unauthenticated |
| User | Any | Authenticated |
| No Access | No Access | No Access |
| Access Point | Network Equipment | Network Equipment |

By keeping the names of the Connection Profiles, Identity Profiles, and Access Policies meaningful and synchronized, matching them up in the Rights Assignment Table should be straightforward. The system in this example would have the Rights Assignment Table show in Figure 2-3.

**Figure 2-3. Right Assignment Table: Example**




- A user that matches the Engineering Identity Profile and the Engineering Connection Profile (which may require an Engineering location and an "Engineering work hours" time window) is given the rights provided by the Engineering Access Policy.
- That same user, if he or she does not match the Engineering Connection Profile (if not connecting at an Engineering location or not during the "Engineering work hours" time window) does not match the first row in the Rights Assignment Table, but does match the second row and is given the rights provided by the Authenticated Access Policy (equivalent to the access allowed in the version 3.1 User group).
- A marketing user is granted the rights provided by the Marketing Access Policy, if they match the Marketing Connection Profile (row 3), otherwise they match row 4 and are given the rights provided by the Authenticated Access Policy (equivalent to the access allowed in the version 3.1 User group).
- Anyone who does not match either the Engineering or the Marketing Identity Profile, but can be authenticated matches the Guest Identity Profile and matches row 6 in the Rights Assignment Table. They are given the rights provided by the Guest Access Policy (equivalent to the access allowed in the version 3.1 Guest group).
- Access Points do not match the Engineering, Marketing, Authenticated, or Guest Identity Profiles, but do match the Network Equipment Identity Profile, so they match row 7 in the Rights Assignment Table and are given the rights provided by the Network Equipment Access Policy.
- Any client that is not yet, or cannot be, authenticated only matches the built-in Any Identity Profile and matches row 8 in the Rights Assignment Table. They are given the rights provided by the Unauthenticated Access Policy (equivalent to the access allowed in the version 3.1 Logon group).

# Test the Migrated System

The 700wl Series system provides a set of tools for troubleshooting rights that can be used to verify the correctness of the migrated system. These tools are:

- The Rights Simulator. This can be used to determine the specific rights that the system gives a specific user connecting through a specific Access Controller port at a specific time.

  To use the Rights Simulator, click the Rights icon in the Navigation bar, then click the **Tools & Options** tab. This takes you to the **Simulate User Rights** page.

- Trace Authentication. This assists in troubleshooting authentication to the system from an external authentication service, such as a RADIUS server. Using Trace Authentication you can find any problems with external authentication.

  To use the Rights Simulator, click the Rights icon in the Navigation bar, click the **Tools & Options** tab, then click the **Trace Authentication** link in the left panel. This takes you to the **Trace Authentication** page.

- Export Rights. You can export the current system rights and compare them with the rights file you created from the version 3.1 system.

  To export the rights to a file, click the Rights icon in the Navigation bar, click the **Tools & Options** tab, then click the **Import/Export Rights** link in the left panel. This takes you to the **Import/Export Rights** page.

  ***Note:*** *Because the rights model has changed dramatically from version 3.1 to version 4, the exported rights files have a very different structure. They cannot be compared on a line-by-line basis.*

# SYSTEM UPGRADE CHECKLIST

# A

This Appendix provides a checklist of the steps required for upgrading the 700wl Series system software from version 3.1 to version 4 and migrating your existing system configuration to the version 4 rights model.

- ☐ **Step 1.** Configure the current 3.1 system for distributed logons and verify that system works properly. (In particular, verify that redirects and allows work as intended.)
- ☐ **Step 2.** Back up the 3.1 system and save the backup file.
- ☐ **Step 3.** Export the rights file, save it to a local file, and print out a copy of the file.
- ☐ **Step 4.** For each of your current locations note the encryption options.
- ☐ **Step 5.** For each of your current locations note the PPTP/L2TP settings.
- ☐ **Step 6.** Get the software update key from HP ProCurve technical support.
- ☐ **Step 7.** Update the Access Control Server or Integrated Access Manager to 700wl Series system, version 4.
- ☐ **Step 8.** Update all Access Controllers to 700wl Series system, version 4.
- ☐ **Step 9.** Verify the correctness of the Configuration settings.
- ☐ **Step 10.** Verify the correctness of the VPN settings.
- ☐ **Step 11.** Create new Authentication Policies.
- ☐ **Step 12.** Create new Identity Profiles, based on the version 3.1 groups.
- ☐ **Step 13.** Recreate any custom logon pages.
- ☐ **Step 14.** Create new Connection Profiles, based on the version 3.1 locations.
- ☐ **Step 15.** Create new Access Policies, based on the version 3.1 groups.
- ☐ **Step 16.** Create new HTTP proxy filters for the new Access Policies, based on the version 3.1 HTTP proxy filters for each version 3.1 group.
- ☐ **Step 17.** Add rows to the Rights Assignment Table.
- ☐ **Step 18.** Test the migrated system.

# FUNCTIONALITY CHANGES

# B

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
  - — An HP Systems MIB that provides information on product type, software version, SNMP notifications, and environmental statistics
  - — An HP-IF-EXT MIB that provides information for each interface on the number of active clients, roaming events, and the number of current sessions
  - — An 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.

# C

# 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 the *Introduction to Software Version 4*.

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)<br>**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:<br>(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<br>**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:<br>Setting up Access Points | **Rights ⇨ Identity Profiles ⇨ Network Equipment ⇨ New Equipment**<br>or<br>**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
5990-8808