The HP ProCurve Secure Access 700wl Series Version 4.1.1.37 Release Notes

Contents

New Features in this Release 2
Documentation 3
System Requirements 3
Upgrade Notes 4
Clarifications and Usage Notes 5
Known Issues and Behaviors 9
How to Get Help 11

Software Version: 4.1.1.37

Part Number: 5990-8811 Edition 1
Date: June 2004

Please go to the support web site located at **http://www.hp.com/go/hpprocurve** for the latest information on the HP ProCurve Secure Access 700wl Series products. The current release notes, manuals, and FAQs are always available at this site.

Important information required for updating system software is available on a secure page at the HP ProCurve web site: **http://www.hp.com/go/hpprocurve**. Click on **Software updates** under the **Product support** header, then choose **700wl series**. Please read the Help information provided for the "Update Software" screen in the Administrative Console before you start to update your system software.

The number in parentheses following a description is an internal tracking number.

NEW FEATURES IN THIS RELEASE

- Multiple administrator accounts. The system administrator can create three levels of multiple administrator accounts providing needed access to the Administrative Console without having to give all administrators full access. The levels are: Network Administrator, Policy Administrator, and Super Administrator.
- Local update. The Local Update option allows software updates of the 700wl Series system from a distribution file stored on the Access Control Server or Integrated Access Manager, rather than from a remote system. This means that a 700wl Series system does not need external (Internet) access in order to obtain the update.
- Export Logs and export Network Equipment list. The ability to export the Network Equipment list, a page of a log, and the complete log file, to a text file is available in this release.
- Access Controller connectivity settings. Once an Access Controller has been installed, changes to the shared secret and Access Control Server IP on that Access Controller can now be made through the Administrative Console.
- Access Controller configuration settings. The configuration settings of an Access Controller are saved in a file on its Access Control Server. Any changes made to an Access Controller while it is disconnected from the network will be overwritten with the saved configuration file once the Access Controller is reconnected to the network. If this is not the intention, then delete the Access Controller using the Access Control Server's Administrative Console before reconnecting it to the network.
- New custom logon templates. The following custom logon templates have been added: Logoff Transition Page, Logon Page Expired Page, and Too Many Attempts Page.
- Redesigned 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.
- Centralized configuration and management. All system components (Access Control Servers and Access Controllers) are managed from the central Administrative Console on the Access Control Server. This includes updating software and viewing system status, including client status and logs. In particular, you no longer need to access individual Access Controllers to manage their configuration or to view client status or logs. The Administrative Console on the Access Controller has been curtailed and is no longer accessible through the 42.0.0.1 URL or the Access Controller IP address.

- New Rights Model. The Rights Manager functions—Authentication and Access Control—have been replaced with a new model that is more logical and straightforward. In the new system, a client is identified in terms of an Identity Profile and a Connection Profile, and this state determines the Authentication Policy and Access Policy that provides rights for that client. The new Rights model is easier to work with than the version 3.1 Rights Manager, and in most cases an equivalent Rights configuration under the new model is simpler and more concise than in the old Rights Manager.
- Access Control Server redundancy and failover. A second Access Control Server can be configured as a redundant peer that will maintain a synchronized, mirrored configuration of the primary Access Control Server. In the event of Access Control Server failure, the secondary Access Control Server can take over management of all connected Access Controllers.
- Remote CLI access via SSH. System components can now be configured to allow CLI access from a remote system via SSH.
- Client-based Bandwidth Rate Limiting. Each Access Policy can be configured with limits for upstream and downstream bandwidth on a per-user basis.
- Enhanced VLAN support. The 700wl Series system now enables the use of separate IP address ranges via DHCP for different VLANs using the port subnetting feature. Use of this feature currently requires that all traffic from the VLAN come into the Access Controller through a single port. Version 4.1.1.37 also supports segregation of VLAN traffic so that a client receives traffic only for the VLAN to which it belongs.

    - Enhanced SNMP support. The 700wl Series system version 4.1.1.37 introduces an additional set of Management Information Bases (MIBs) that can provide statistical and state information on the 700wl Series system. The latest version of the 700wl Series system MIBs is available on the HP ProCurve support web site at http://www.hp.com/go/hpprocurve.

DOCUMENTATION

Documentation is available through the Online Help feature in the Access Control Server Administrative Console. Click the Help button to display context-sensitive Help about the page you are viewing. From the Online Help interface you can navigate within the Help system to find topics of interest, and you can access the complete *HP ProCurve Secure Access 700wl Series Management and Configuration Guide* in PDF format.

Documentation is also available on the HP ProCurve Technical Support web site at **http://www.hp.com/go/hpprocurve** and may be updated as the need arises. It is recommended that you check the web site periodically to view the most current information about the product.

SYSTEM REQUIREMENTS

- For software release 4.1.1.37 the following client browsers have been fully tested and are supported for use with the Adminstrative Interface:

Operating System	**Browser Software**
Windows XP	Internet Explorer 5.5 with Service Pack2

Windows 2000	Netscape 7.1
RedHat Linux	Netscape 7.1 Mozilla 1.5
Solaris	Netscape 7.0 Mozilla 1.2.1
Mac OS X	Internet Explorer 5.0* for OS X

Internet Explorer for OS X cannot interpret the up/down arrows on some of the pages in the Administrative Console, and does not uncheck a checkbox when its corresponding alternative is checked. (4876)

Other browsers, such as earlier versions of Internet Explorer, earlier version of Netscape, or Safari (Macintosh) may not display all pages or data correctly.

UPGRADE NOTES

Important: Please read *Upgrading 700wl Series Software V3.x to V4: A Guide to Methods and Concepts* for instructions on upgrading and modifying your rights to work with the new Rights model **before** you do the upgrade.

Important: Upgrading from software release 3.1 requires that you recreate your rights configuration with the new Rights model. While many of the components used within the Rights Manager are migrated from version 3.1 (such as your Allows and Redirects, Authentication service configurations etc.) your Location and Group configurations are not migrated. Instead, you must create Connection Profiles, Identity Profiles, and Access Policies, which replace the functionality of Groups and Locations. In most cases an equivalent Rights configuration under the new model is simpler and more concise than in the old Rights Manager.

For an introduction to the new release 4.1 user interface as it compares to the version 3.1 interface, see the *Introduction to Version 4*. These documents may be downloaded in PDF format from the HP ProCurve Technical Support web site at **http://www.hp.com/go/hpprocurve**.

Important: Back up your systems before upgrading to the version 4.1 software!

- In the 3.1 software, the names for the 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. (5075)

- An upgrade to version 4.1 is supported from release 3.1.122 or later. If you are running earlier releases of 3.1 it is recommended that you upgrade to the current 3.1 release (currently 3.1.128) before you upgrade to version 4.1.
- Both the Access Control Server and any Access Controllers to be managed by this Access Control Server must be upgraded to version 4.1. Interoperability between version 3.1 and 4.1 software is not supported.
- In version 4.1, Centralized logon is no longer supported. In version 3.1 Distributed logon was the default, but Centralized logon was still supported. If you are running software

version 3.1 and have not converted to Distributed logon, you should do so, and ensure that logons are working properly in Distributed mode before you upgrade to version 4.1.

- If you maintain an Access Control Server running version 3.1 in parallel with an Access Control Server running version 4.1, and you migrate an Access Controller from the 3.1 Access Control Server to the 4.1 Access Control Server, the 3.1 Access Control Server may continue to try to contact the previously in-service Access Controller. This may result in error log messages on the 3.1 Access Control Server. These messages are benign and may be ignored. (4426)

CLARIFICATIONS AND USAGE NOTES

The following items assist you in configuring and operating your system with this software version. The number in parentheses following the description is an internal tracking number.

- In an SNMP MIB walk on an Access Control Server, the following additional variables are listed in the HP-IF-EXT MIB file:

  hpifMIBObjects.2.1.1.1.1 Gauge 0

  hpifMIBObjects.2.1.1.2.1 Gauge 1

  hpifMIBObjects.2.1.1.3.1 INTEGER 0

  hpifMIBObjects.2.1.1.4.1 INTEGER 0

  This additional information does not affect system operation. (5572)

- In the "Management and Configuration Guide," the manual states incorrectly the name of the software distribution files to download from the HP ProCurve Technical Support web site for the Local Update feature. For an Access Control Server or Integrated Access Manager, the correct distribution file to download is "740wl-760wl-dist-4.1.1.37." For an Access Controller, the correct distribution file is "720wl-dist-4.1.1.37." (5568)
- When uploading a distribution software image file through the Local Update tab, select a row in the Uploaded Software Versions table before performing the upload. (5450)
- If a redundant system experiences a failover and the administrator makes configuration changes to the acting primary Access Control Server (previously the secondary), those configuration changes will be lost when control is returned to the original primary Access Control Server. Therefore, if a failover occurs, diagnosing and repairing the problem with the primary Access Control Server should be performed before any configuration changes are made. (5380)
- When creating or editing filters for Allowed or Redirected traffic and using a "!" or the word "not" in front of the address, you must include a space between the "!" or the word "not" and the address. For example: not @internal@. (5301)
- The CLI command, "get mindowngrade," applies to the minimum compatible version of software for the unit with regards to internal data structures, not for software compatibility with other components in the 700wl Series network. (4211)
- If the Access Control Server has previously recognized an Access Controller, any changes made to the Access Controller while it is disconnected from the network will be overwritten with the saved configuration file stored on the Access Control Server once the Access Controller is reconnected to the network. If this is not the intention, then delete the Access Controller using the Access Control Server's Administrative Console before reconnecting it

to the network. However, it is recommended that the Access Control Server handle all Access Controller configurations.

- Clients running Windows XP and using L2TP/IPSec or IPSec VPN to authenticate need to disable the Internet Connection Firewall (ICF) service. If ICF is enabled, the client's connection will be dropped when the IPSec security association has expired. (5248)
- Clients running Windows 98 that have logged off, or have been logged off automatically, need to wait 20 seconds before logging on again. This is a Windows 98 constraint. (4833)
- Displaying the status of the primary or secondary Access Control Server while they are synchronizing may result in either an error message stating "DB Error: connect failed" or "Page data is invalid." This only occurs in redundant systems with unusually high configuration activity. If this error message does occur, click the Back button on the browser to clear it. (5221)
- After changing the time zone on a 700wl Series component, it takes approximately seven seconds for the new time to take effect. (5243)
- Before merging two 700wl Series system networks together to create a redundant system, where both Access Control Servers are active, first deactivate the Access Control Server that is designated to be the secondary Access Control Server in the redundant system. (5247)
- With version 4.1.1.37, the management of all 700wl Series components, including configuration and management of all Access Controllers associated with the Access Control Server, is done centrally from the Administrative Console on the Access Control Server. Because of this, the ability to configure an Access Controller directly has been curtailed:
    - The Administrative Console on an Access Controller is no longer accessible by pointing a browser to the IP address of the Access Controller, or to the 42.0.0.1 address. In either of these cases, you are presented with the Administrator Logon window, but when you complete the logon you are presented with a page that provides a redirect to the Access Control Server (or allows a logout).
    - The Command Line Interface on an Access Controller provides a limited number of commands, allowing configuration of only the basic parameters necessary to enable the Access Controller to communicate with its Access Control Server (IP address and shared secret). It does provide commands to enable viewing of the status of the unit, as well as certain other functions such as the ability to upgrade, backup, shutdown and restart the unit.
- There are a number of functions that will result in termination of an active SSH session. These include any CLI commands (or the equivalent function done through the Administrative Console) that cause a global restart, such as changing the NAT DHCP settings, enabling or disabling remote access, enabling or disabling SSH under Wireless Data Privacy Setup, or changing the Access Control Server IP address. Any of these actions cause the system to restart internally which shuts down any open SSH sessions.
- A user that logs on as "Guest" matches the Guest Identity Profile, but is not considered to be an authenticated user. If the Guest Identity Profile is associated with a Connection Profile that includes a time window, and the time window expires, the Guest user will then default to the Any Identity Profile and presumably gets rights based on the "Unauthenticated" Access Policy. On the other hand, a Registered Guest is an authenticated user, because its name and password are in the user database, although it is assigned to the Guest Identity Profile. In this case, if the Connection Profile associated with the Guest Identity Profile expires, the

Registered Guest will match the default “Authenticated” Identity Profile and get rights based on the Access Policy associated with that Identity Profile. (4538)

- Using a Cisco VPN client with Extended Authentication, and with IPSec enabled in the Access Policy, the client is unable to browse to the 42.0.0.1 address. This is because in this particular case the client attempts to use the 42.x.x.x outer tunnel address rather than sending this traffic through the IPSec tunnel. (4575)
- If you configure an IP address range for VPN tunneling (via the IP Address Assignment page under the VPN icon) you must also set “Allow Static IP” in the relevant Access Policies (including the Unauthenticated Access Policy). (4702)
- In a configuration with multiple Access Controllers, with all ports configured to use real IP addresses, if a client connects to a port that has been configured with a port subnet range, the client will receive a real IP address within that range. If that client then roams to an Access Controller that does not have that subnet range configured, no traffic will be passed for that client. This is because there is no routing information on the new (roamed-to) Access Controller for the port subnet range. The client will eventually time out and receive a new real IP address from the common pool on the roamed-to Access Controller, and will then be able to pass traffic, even after it roams back to the first Access Controller. This problem can be avoided by configuring the same port subnet range on every Access Controller that a client might roam to. The subnet range can be configured on any port on the Access Controller -- even a port that is not active. Just adding the port subnet is sufficient to get the proper routing information created.
- Access Points should be configured to get a real IP address via DHCP, rather than using their default IP address. If the default IP address conflicts with one of the 700wl Series system internal addresses, the AP may not reliably stay connected to the system.
- There are several issues related to using IPTV multicast streams:
  - The IPTV stream may not stop immediately when the client is logged out. This is as expected due to the IPTV protocol. (4664)
  - If multiple clients are using the same IPTV stream, the stream will continue for users that log out as long as one client using the same stream remains logged in. (4665)
  - Multicast streams such as IPTV and VPN tunneling (IPSec, L2TP, or PPTP) are incompatible. Multicasting will not work for clients using VPN tunneling. (4667)
- When using NT Domain Logon, if a client is unable to contact the NT Domain Server immediately, for example if it has yet to receive an IP address, the client will resort to a cached logon. However, a cached logon cannot be sniffed, so the 700wl Series system will not detect that the client has logged on, even though the NT logon appears to succeed on the client. It is possible to work around this problem by disabling cached logon through the Windows registry. This can be accomplished by setting `My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon\cachedlogonscount` to "0" (zero).
- The HP ProCurve Secure Access 700wl Series products require version 3.0 or greater of the Network Time Protocol (NTP). Be sure your NTP server is running version 3.0 or greater, and verify that you have IP connectivity from the 700wl Series product to your NTP server.
- If you change the uplink port, you must reboot the device before you can access the device's web interface again.

- If an administrator's or client's browser fails to successfully negotiate an SSL connection with the 700wl Series system's web server, the OpenSSL subsystem will place some fairly obscure messages in the logs. You can identify these errors by their references to OpenSSL or to RSA key errors. These errors are harmless as the browser and server generally do eventually succeed in establishing an SSL connection.
- The SafeNet 7.0.x client in combination with Windows XP does not allow roaming. A roam away from the initial Access Point causes the interface to go down, and the SafeNet 7.0.x client cannot recover. A client reboot is required before you can connect again. Roaming works correctly with the SafeNet 9.0.x client. Roaming also works with the 7.0.x client and other Windows OS versions.
- Using 802.1X and the Odyssey client, when a user that has been successfully logged on disconnects and is logged off, and then tries to reconnect immediately by checking the "Connect" option, the second logon is not successful, because the client assumes it is reconnecting to an already authenticated connection. The client must use the "Reauthenticate" option to reconnect in this case. (3319)
- Orinoco WaveLAN cards used with Windows XP do not allow successful roaming. This is because when an Orinoco-enabled Windows XP system associates with a new Access Point, the associated driver forces the interface to go down, destroying all open sessions. The client should still get the same IP address, but all sessions will be gone. (2665)
- If you need to modify the 700wl Series system bridging options through the Advanced Network Configuration page under the Network Setup tab, you should do so when the system is idle. When you change bridging options, any clients logged on to the system are logged off. However, they are not completely logged off – client connections are dropped, but the clients are not removed from the Client Status list on the Access Controller. For each client connected when the bridging option was changed, there will be error entries in the log file similar to the following:

  ```
  Error 00:20:e0:8d:d8:91: write: Socket is not connected
  Error ambit_ngcfg_disconnect_hook: can't disconnect ip hook: Bad
  filedescriptor
  ```

  These clients will not be able to log on again, because the system thinks they are still logged on. The workaround has two parts:

  - From the Client Status display, log out the client.
  - The client must release and renew their IP configuration. They will then be able to log in.

- The 700wl Series system supports SecureCRT 4.05 with the Auto Detect or Standard SSH server options. It does not support SSH Communications 2.1.0 or 2.3.0, or DataFellows 2.0.12 or 2.0.13. (2739)

- The 700wl Series system does not support the Phase 2 Compression (Deflate) option with the SafeNet SoftRemoteLT client. You must disable this feature in order to establish a connection.

KNOWN ISSUES AND BEHAVIORS

The following are issues that are known to exist with this software version. The number in parentheses following the description is an internal tracking number.

- When creating a new RADIUS Authentication Service use the IP address of the RADIUS Server for the Server field. Currently, the option to enter the Fully Qualified Domain Name (FQDN) does not work with RADIUS Authentication Service. (5549)
- A user name can be added with the same name as an existing Identity Profile, but an Identity Profile name cannot be added with the same name as an existing user. (5528)
- The special characters, ampersand (&), less than (<), greater than (>), and quote (“) are not recognized correctly in an Authentication Policy name and all clients using an Authentication Policy with the aforementioned special characters will not be able to get access rights. (5526)
- In extremely rare circumstances, Access Controllers may not complete an administrator initiated reboot and remain in a continuous reboot state. If such a condition exists:
    - First disconnect all the devices plugged into the downlink ports of the Access Controller for a few minutes. When the reboot cycle completes, reconnect the devices to the downlink ports.
    - If the above procedure does not solve the issue, perform a factory reset of the Access Controller by connecting to the Access Controller through the console port and immediately typing “**F**” when the "To initiate a factory reset, press 'F' now..." prompt is displayed. There is a three-second timer to respond to the prompt during the reboot process. For more information, see the *Command Line Interface* chapter in the *Management and Configuration Guide*.

  As a factory reset clears any existing configuration information in the Access Controller, it is advisable to write down any configuration information about the Access Controller prior to performing an administrator initiated reboot operation. Please note that Access Controller specific configuration information is limited only to DHCP, IP address, hostname, DNS, and interface IP information. All rights information including identities, access policies, users, connection profiles, and such are stored on the Access Control Server. (5513)
- Currently the NAS-Identifier is not sent with Transaction Tracer or User Rights Simulator packets. Some RADIUS servers, such as the Merit AAA Server, require either the NAS-Identifier or the NAS-IP-Address for all packets sent to the server and will refuse packets that do not contain this information. (5503)
- In a redundant system, uploading a large DIST file over a slow connection to the primary may cause a failover. (5456)
- Modified Logon Customization on imported rights will not take affect until the Access Control Server is rebooted. (5412)
- Remote CLI access via SSH allows network administrators all the rights of a super administrators. (5407)
- Clients using LEAP authentication and identified with an Access Policy that requires DHCP for IP address assignment may experience network connection problems even though they have received a real DHCP IP address. The workaround is to specify the IP address of the DHCP Server in the Access Controller Network Basic Setup tab. (5401)

- In an Integrated Access Manager, sometimes the connection time displayed for the internal Access Controller is one minute greater than the Integrated Access Manager's total uptime. (5399)
- In the Access Policy Timeout tab, the "Force users to reauthenticate at a fixed time of day" is currently not functional. (5397)
- In the Access Policy Timeout tab, the Linger Timeout field accepts negative integers when it should only accept positive integers. The Reauthenticate field allows entry of alphanumeric characters but will not save them. The Reauthenticate field should only accept positive integers. (5384)
- Clients using a real IP address with L2TP or PPTP authentication that are authenticated through an Access Controller connected to a Cisco Catalyst 2950 have their IP address associated with that Access Controller by the Catalyst 2950. If the clients log out and attempt to log in again to another Access Controller connected to the same Cisco Catalyst 2950, or roam to another Access Controller connected to the same Cisco Catalyst 2950, they will not be able to gain network access because the Cisco Catalyst 2950 associates the client's IP address with the first Access Controller. Clearing the ARP cache on the Cisco Catalyst 2950 removes the previous association of the client's IP address with the first Access Controller and allows the client to connect through the other Access Controller that is connected to the same switch. (5323)
- When redundancy is disabled in a redundant 700wl Series system, the secondary Access Control Server reboots but sometimes does not complete a factory reset. When the former secondary Access Control Server reconnects after rebooting and not completing a factory reset it sends a message to all Access Controllers in the system identifying itself as the secondary Access Control Server. If the former primary Access Control Server is rebooted, the Access Controllers will attempt to connect to the former secondary Access Control Server. (5242)
- Several minor error messages or minor information messages are added to the log when a client attempts to access a restricted page. (5284)
- Downgrading to a prior release may cause known issues of the earlier version to re-emerge. If downgrading to a prior release in a redundant system, disable redundancy before performing the downgrade. (5215)
- The LCD display on the Access Controller may blank out when throughput is high. (5188)
- The "Maximum Concurrent Logons per User" setting in an Access Policy does not apply to sessions using SSH port forwarding. (1708)
- In the Network Setup page, providing a hostname of more than 50 characters creates errors in the log, and the name is not properly resolved. (2829)
- From the CLI, doing a traceroute command on an invalid IP address gives only a partial result and does not appear to complete. The workaround is to press Return after waiting at least 30 seconds (the traceroute timeout interval). (3176)
- When bandwidth rate limiting is enabled in an access policy, several behaviors should be noted:
    - When both the upstream and downstream limits are configured the same, the downstream throughput is consistently slightly greater than the upstream throughput. (3115)

- When the bandwidth limit is set to one of the lower limits (56K or 128K) the throughput can temporarily exceed the configured limits when the traffic stream first starts up. The throughput settles to within the configured limits within a few minutes. (3272)
- For TCP streams, if IP options are present (not the normal case) the bandwidth limiting function does not account for these options correctly, resulting in poor TCP shaping. (3325)

- The HTTP Proxy feature was implemented using HTTP 1.0. Sites that make use of HTTP 1.1-specific features may not work reliably. In particular, clicking on a link may result in the browser being redirected to various erroneous alternate links. (3557)
- The new bandwidth limiting feature, when used with a tunneled protocol such as L2TP with IPSec, will typically provide throughput somewhat lower than the configured limits. The throughput will vary with the worst case being a passthrough VPN, or the case where the client has roamed and the traffic is tunneled between Access Controllers. In the worst case the bandwidth can be as low as 30% of the configured bandwidth. (3830)
- When viewing Client Status from the Access Control Server for all Access Controllers, some clients may be displayed with blanks as the IP address. This may happen through both the Administrative Console or through the CLI. To see the actual IP address assigned to the client, you can take one of two actions:
  - Display the detailed view for the client
  - Select the Access Controller through which the client is connected, and display client status just for that Access Controller.

  In either case, the IP address will then be displayed correctly. (4651)

How to Get Help

Visit the HP ProCurve Networking web site at **http://www.hp.com/go/hpprocurve**. Click on **product services** for information on available support resources and options for contacting HP.