Release Notes
Version 3.1
HP ProCurve Secure Access 700wl Series

Integrated Access Manager 760wl
Software Release **3.1.128**
Release Notes Part Number 5990-5986 Edition 5

Build date: Apr 24 02:15:10 2004
Install date: Jun 24 13:45:08 2004

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, FAQs, and problem reports are always available at this site.

These release notes describe the known issues for the current release of the HP ProCurve 700wl Series software. Release numbering is defined as x.y.z, where x is the major release, y is the minor release, and z is an internal build number.

Note: HP strongly recommends that you create and save a backup before you upgrade to a new release.

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 Interface before you start to update your system software.

Contents

What's New in this Release

Installation and Usage Notes

Software Fixes

Known Problems

How to Get Help

What's New in this Release

Release 3.1 adds several product features and fixes a number of bugs.

Ability to lock in port settings

Through the Advanced Network Configuration page, you can now specify the port setting (media type and options) for downlink ports and the uplink port. An abbreviated form of the Advanced Network Configuration page is now available on the Access Control Server 740wl so that you can configure the port setting for the uplink port.

Retrieval of MAC Address User information from LDAP repository

A new feature enables the HP ProCurve 700wl Series to retrieve MAC addresses from an LDAP repository, and add them to the built-in database as MAC address users on a regularly-scheduled basis. You can also retrieve group membership information for these users if that information is kept in the LDAP repository.

Minor Enhancements

Guest group default access rights made more restrictive

In software versions prior to 3.1, the predefined Guest group included the "Outside World" Allow, which allowed access to any IP address except the subnet defined for the Access Control Server 740wl. This allow is no longer enabled by default for the predefined Guest group. Thus, in the default case, Guest users will not have any network access after they log on. Guest group rights will need to be modified to provide an appropriate set of rights for Guest users. See Chapter 7, "Configuring Groups" in the HP ProCurve Secure Access 700wl Series Management and Configuration Guide for information about modifying a group's access rights.

Note that this will not affect existing Guest groups upgraded from an earlier version of the software, unless a Factory Reset is performed.

DHCP address range for NAT now configured centrally

The DHCP address range used for private addresses for NAT clients is now configured on the Access Control Server 740wl rather than on each Access

Controller 720wl. This ensures that one address range is enforced across all Access Controller 720wls.

Installation and Usage Notes

Following are some general notes pertaining to product installation and usage.

- When using NT Domain Logon sniffing for authentication, the HP ProCurve 700wl Series cannot detect a logoff from the NT domain. When an NT domain user logs off, that user's rights will remain in effect until the Access Controller 720wl detects that the user is no longer connected and the Rights Manager linger timer expires. If another user logs on from the same client before this has happened, the first user's session accounting information is maintained. If the first user had roamed and had sessions tunneled back to another Access Controller 720wl, the second user's sessions will also be tunneled to the original Access Controller 720wl. The workaround is to log the client off via the Administrative Interface.
- The interaction between DHCP relay packets and VLAN tagging behaves as follows:
    - DHCP relay packets leave the Access Controller 720wl untagged regardless of client VLAN tagging (this occurs when an external DHCP server is configured).
    - Relayed DHCP broadcasts (these occur when the DHCP Server IP field is blank) are always tagged.
- In a configuration with multiple Access Controller 720wls, 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 720wl 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 720wl 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 720wl, and will then be able to pass traffic, even after it roams back to the first Access Controller 720wl.

  This problem can be avoided by configuring the same port subnet range on every Access Controller 720wl that a client might roam to. The subnet range can be configured on any port on the Access Controller 720wl -- 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 HP ProCurve 700wl Series internal addresses, the AP may not reliably stay connected to the system.

- 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 HP ProCurve 700wl Series 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 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 HP ProCurve 700wl Series product to your NTP server.
- VLANs are not necessary when using downlink ports on the HP ProCurve 700wl Series. HP recommends that you do not use VLANs because it limits the ability to take advantage of the Rights Management capabilities of the HP ProCurve 700wl Series products.
- Using auto-configuration scripts in your web browser with the HP ProCurve 700wl Series causes the browser session to hang because access to the script server requires you to log in to the network first, but your browser will not let you log in without accessing the auto-configuration script. The use of browser auto-configuration scripts is not recommended with the HP ProCurve 700wl Series products.
- As of Version 3.1, there is a maximum limit for the built-in user database of 5000 users. This limit is enforced when you attempt to add users through the User Editor.
- The Import Rights function limits the size of the Rights image file to 2.5 Mbytes. In most cases, given a 5000-user limit for the built-in user database, this should be more than sufficient. However, there is no limit to the size of the export file.
- In general, Netscape 6.x versions do not work well with the administrative interface. Formatting of the HTML is often not quite correct and other issues have been noted.
  Netscape 4.79 or earlier versions are not supported.
- There is a known problem with SSL in older Microsoft Internet Explorer versions. Ensure you are running the latest patches for MSIE.
  Similarly, there are known problems with SSL and the Mac OS/X default browser. Ensure you are running the latest version of the Mac OS/X browser.
- The Mozilla/Netscape(6/7) browser caches the SSL certificate/key, and does not automatically delete it when it changes. If you perform a function on the HP ProCurve 700wl Series that causes the certificate to be regenerated, such as a Factory Reset or changing the host name, the Mozilla browser will display an alert stating that it has received an

incorrect Message Authentication Code. You must restart the Mozilla/Netscape browser to clear the old key/certificate.

- The HP ProCurve 700wl Series supports SecureCRT 3.3 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.
- The HP ProCurve 700wl Series 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.
- Roaming from subnet to subnet with a PPTP or L2TP connection is not as efficient as roaming with a non-encrypted NAT connection. All traffic must be tunneled back through the original Access Controller 720wl when roaming with PPTP or L2TP.
- The IPSec software in this release can be excessively "chatty", producing voluminous output regarding IPSec connections. In general this is useful for debugging troublesome connections, but it can sometimes appear that errors are being reported when everything is working properly.
- Access Controller 720wls have the software image stored in solid-state flash memory instead of on disk. This means there are two different software images, one for Access Controller 720wls and one for disk-based units. Access Controller 720wl software versions have "-am" appended to the filename. It also means that internal logs on Access Controller 720wls are cleared upon reboots.
- It is now possible to install an Access Controller 720wl by setting all network installation parameters by means of a DHCP server, if the DHCP server is configured to support this. See Appendix B of the HP ProCurve Secure Access 700wl Series Installation Guide for information on configuring a DHCP server to support this feature.
- If you change the uplink port, you must reboot the device before you can access the device's web interface again.
- In this version of the software, if a client is a member of multiple groups with different expire times, a restrictive expire time (either relative or fixed) always takes precedence over the NEVER expire setting. If the client is a member of multiple groups, each with relative expire times defined, the longest expiration interval takes precedence. See Chapter 6 in the HP ProCurve Secure Access 700wl Series Management and Configuration Guide for a detailed explanation of how Expire Time settings work. This behavior is different from software Version 2.0, where an expire time of NEVER would override a more restrictive expire time.
- In some situations NT Domain login will fail if a client wants to do a NetBIOS request to both the WINS server and the Domain Controller, but the WINS server is not the same as the Domain Controller. The reason is that by default *all* NetBIOS requests (to port 137) are redirected to a single server. To work around this, create a second redirect that redirects the specific NetBIOS request to the WINS server. For example, if the WINS server is 192.168.1.255, then redirect 192.168.1.255:137 to 192.168.1.255:137. Be sure you give this redirect a name that is

alphabetically "higher" than "netbios-ns", such as "alt-netbios-ns", as the order of processing is in alphabetical order by the name of the redirect.

- VPN clients with Perfect Forwarding Secrecy (PFS) enabled in their IPSec configuration will not be able to establish a connection with the HP ProCurve 700wl Series.
- In order to support VPN clients using IKE Aggressive mode, the IKE Diffie-Hellman setting on the IPSEC Configuration page must be set to use only one Group. This will allow clients using either IKE Aggressive Mode or IKE Main Mode with the specified group to connect. The Windows L2TP/IPSEC client does not support Group 5, so in this case you must select either group 1 or group 2.
- When using the Microsoft IPSec VPN client with Windows 98SE or Windows ME, after creating a new Dial-Up Networking Connection, you must go to the Properties for that connection, display the Server Types page, and disable (uncheck) "Software Compression" which is enabled by default.
- If an administrator's or client's browser fails to successfully negotiate an SSL connection with the HP ProCurve 700wl Series's web server, the OpenSSL subsytem 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.
- When the IP address of the Access Control Server 740wl or Integrated Access Manager 760wl changes, if a client request occurs before the IP address change process has completed, a "Device not configured" error message may appear in the log (such as `Error http_server: XML-RPC: handler for "setRights" failed: Device not configured`). An IP address change may occur on the Access Control Server 740wl or Integrated Access Manager 760wl upon bootup if the system is configured to use DHCP to get its address. This can also occur when an administrator changes the IP address through the Administrative Interface. This message may be safely ignored.
- 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.
- 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 HP ProCurve 700wl Series bridging options through the Advanced Network Configuration page, 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, in versions 3.0 and later, they are not completely logged off -- client connections are dropped, but the clients are not removed from the active clients list on the Access Controller 720wl. 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 file descriptor
```

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 Active Clients list on the Access Controller 720wl, log out the client.
- The client must release and renew their IP configuration. They will then be able to log in again.

- Using Netscape version 6.1 to access the administrative interface results in a "pause" of 1 minute the first time you access the administrative interface. This is a known problem with Netscape 6.1 and has been reported to Netscape.
- Using Microsoft Internet Explorer version 5.1 for Mac OS/X, rights exported from the Rights Manager cannot be imported, but generate an error. MSIE versions 5.1.4 or later appear to work correctly.

Software Fixes

The following problems have been fixed since version 3.1 was released. The number in parentheses following the description is an internally-maintained tracking number.

The following problems have been fixed in the current maintenance release:

- External Group Retrieval is now working for Active Directory LDAP. (5273)
- The Fiber Optic Option Card, 1000BaseSX/LX, and the Ethernet Option Card have been improved and require the 3.1.128 release or higher. If you ordered one of these cards after October 2003, then you will need Release 3.1.128. (5235)
- Under RedHat Linux (and possibly in other cases) packets that exceed the MTU size are transmitted in reverse order, and these packets were being dropped. This has been fixed. (4705)

The following problems were fixed in maintenance release 3.1.122:

- With Microsoft 2003 Server, some users using the HP ProCurve 700wl Series Kerberos authentication service, were unable to log on, and an error message would appear in the logs in the form error: KRB52. This has been fixed, so these users can now logon successfully. (3537)
- In situations where clients were using unencrypted RPC_NETLOGON packets to log on to Windows domains, the HP ProCurve 700wl Series could not sniff the logon packets, and would not recognize the logon. This was observed with a Windows NT 4.0 domain controller server. This has been fixed. (3656)
- Entering an @ sign in a logon name when using Kerberos authentication would always allow a user to successfully log on. This has been corrected so that an @ in the logon name will result in the authentication request failing. (3723)
- A customized logo configured for the small browser version of the logon page was not being rendered on an iPAQ. (3527)
- The Auto-Proxy would fail to return pages if error messages were injected directly into the HTTP header by the originating server. (2997)
- There were several situations under which DHCP lease renewal requests would not be successful:
    - If you are using the port subnet feature (configured via the Advanced Network configuration page), and a client connected through that port attempted to renew its DHCP lease using a unicast renew message, the unicast renew message would be unsuccessful. This caused "unexpected DHCP DHCPACK" log messages.
    - If the DHCP lease time was very short (at or below two minutes) both unicast and multicast DHCP requests/discovers might cause an incorrect session entry to remain in a client's session table.

  Both these issues have been fixed. (3202).

- The IPSEC code did not handle tunneled large (> MTU size) UDP or ICMP packets properly, resulting in memory corruption. The system would panic and systems without console access would appear to be hung indefinitely. The problem has been corrected by checking for this condition and allocating a new mbuf for IPSEC processing. (3109)
- NT Domain logon sniffing would fail to detect a successful NT Domain logon, if IPSec was enabled on the client and the client had roamed away from the Access Controller 720wl that it originally associated with. This has been fixed. (3097)
- For Groups that used the "EveryOtherTime" When (the default) the Rights Manager was not detecting that the "Members of this group do not get Implicit User rights" option was checked, and the group would always grant Implicit User rights to group members. This has been fixed. (3095)

- Clients that requested Real IP-mode DHCP leases through a downlink port that was configured with a port-subnet (through the Advanced Network Settings page) could receive an incorrect DHCP address from the wrong subnet, or no address at all, depending on the DHCP server configuration. This was because the DHCP Request's GID field was not being rewritten with the configured downlink port-subnet. This has been fixed. (2955, 2959)

The following problems were fixed in maintenance release 3.1.111:

- Memory leaks in the IPSec implementation related to Security Associations (SA) would cause IPSec error messages similar to the following:
  ```
  Error IPSec: pfkey UPDATE failed: No buffer space available
  Error IPSec: pfkey ADD failed: No buffer space available
  ```
  Eventually clients using IPSec would lose the ability to connect to the network through the Access Controller 720wl, making a reboot of the unit necessary. This has been fixed. (2922)
- When a Windows-based client using a real IP address roamed to a different Access Manager and then experienced an abnormal shutdown (e.g. lost power, hung or crashed requiring a reboot) such that the DHCP lease was not released, after rebooting the client would not be able to get network access. This problem has been fixed. (2898, 2903)
- If there were clients logged in as Registered Guests when a "Refresh every client's rights" action was done from the Rights Manager Clients page, the Registered Guest clients were being refreshed with default User rights (typically meaning they got unrestricted access and no login expiration) rather than Guest rights. This has been fixed so that Registered Guests continue to receive Guest rights after rights are refreshed. (2899)

Known Problems

- There are interoperability issues using the web proxy BlueCoat (aka CacheFlow) version 4.1 with the HP ProCurve 700wl Series products.

  The following proxy servers are compatible with the HP ProCurve 700wl Series products:
  - Netscape Proxy Server
  - Microsoft Proxy Server
  - Multi-Proxy
  - Anonymity 4Proxy
  - Linkbyte Proxy Server
  - Squid 2.4 on Solaris 8

If you are having problems getting through your web proxy server verify that your web proxy server is one of those listed above. (2904)

- The CLI does not configure copper Gigabit Ethernet option cards correctly. Use the Administrative Console to configure these cards. (5333)
- Using web-based logon against a Kerberos server (2003 Advanced server) entering a blank (" ") as the user name with no password logs on the client as a Guest. (3777)
- The Auto-Proxy will sometimes fail to restart itself if many connections to non-existent websites are made. (3333)
- Under Advanced Network Configuration, when setting a port subnet range for a port, it is possible to select the netmask "224.0.0.0 (/3)" but it generates an error and the setting is not applied. (3070)
- The Automatic 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 numerous erroneous alternate links. (3557)
- If Automatic HTTP Proxy is configured for a group, and a client member of that group has configured its web browser to use 42.0.0.1 (ports 80 or 8080) as its proxy server, that client will not be able to browse. 42.0.0.1 should not be used as the proxy server address. (3539)
- If you configure and enable HTTP Proxy Filtering for a group, and then create a duplicate of that group by changing its name and submitting changes, the new group will not be configured to use the HTTP proxy filters of the original group. HTTP Proxy filtering is disabled for the duplicate group, no ports are configured, and the only filter is "deny all." You must configure the new group with HTTP proxy settings to duplicate the settings of the original group. (3142)
- In distributed mode, when using the Registered Guest feature, the Username and Password are added to the Rights Manager built-in database, but no Log file entry is created. Therefore, it is not possible to retrieve the information in the First Name or Last Name fields. This was fixed in an earlier version of release 3.1 but no longer works correctly. (2632)
- If a small DHCP IP address range is specified for NAT (in the DHCP Network for NAT Clients area on the Advanced Network Configuration page) the NAT DHCP server may start assigning duplicate IP addresses, resulting error messages saying that the address is already in use. The workaround is to increase the address range to allocate a larger subnet space, so that the liklihood of collisions is reduced. (2862)
- When using RADIUS accounting, occasionally an error message may appear in the logs indicating that the "Sniffer process died." When this occurs the Sniffer process automatically restarts, but no corresponding restart message appears in the logs. (2752)

- On a HP ProCurve 700wl Series that is set to "Encryption Allowed but not Required", if a user connects using an IPSec VPN client (rather than a PPTP or L2TP VPN client) and then turns off IPSec, even before logging on, the IPSec termination point is not closed down. The client will then not be able to log on. There are three ways to fix this:
    - The client can reenable IPsec, log on and then log off
    - The Administrator can log the client off via the Administrative Interface
    - The user can shut down his system, and wait until the system logs the client off when the linger timer expires. (2625)
- If a client currently associated with one wireless access point roams to a new access point, but does not send any packets to the network through the new location, the Access Controller 720wl will not know that the client has moved. In particular, if the client was receiving packets from the network in the old location, the connection will appear to "freeze" as the previous Access Manager will be unaware of the new location of the client. A workaround is to ensure at least one packet is sent back into the network from the new location. (475)
- It is important that the system time of day be kept accurate, and the time should not be set backwards while the system is in operation. A backwards change in the time of day (either manually or via NTP) will cause the system time to appear frozen. It will advance again when the difference between the original time and the new time has elapsed. (For example, if the time is set back one hour, the original time will continue to be reported as the current time until one hour has elapsed.) This may also cause some internal timeouts to take longer than normal. In addition, odd information may be displayed by the Rights Manager in that previously expired and logged off users can be made to appear active, until the system moves beyond the time these users logged off or had their rights expire. Therefore, if a backwards time change is necessary it should be done during times when system usage is low to minimize any possible disruptions. Rebooting the system will set the system time correctly. (536)
- When a Windows XP client connects to a location that allows real IP and PPTP or L2TP/IPSec, and then roams to another Access Controller 720wl, the IP Security setting for the client is displayed incorrectly in the Client Information page on the new "roamed to" Access Controller 720wl.
  - For L2TP/IPSec, the reference to L2TP will not appear; only the IPSec information is displayed. (1656)
  - For PPTP, the IP Security setting on the roamed to Access Controller 720wl is displayed as "None" (2319)

  In both cases the actual security is maintained correctly.
- Setting the clock backwards causes the LCD display to freeze until the clock passes the time displayed on the LCD. (2387)
- It is possible for multiple users to log in via the browser-based interface, with unique user names, but then all establish SSH sessions using the same SSH user ID, even if the "Max # of concurrent logins" limit for the

group is set such that this should not be possible. When a client attempts to establish an SSH session in violation of this limit, the Access Control Server 740wl or Integrated Access Manager 760wl denies the logon request (and its log entries reflect this) but the Access Controller 720wl allows the session because it identifies the client as already logged on under its original (unique) logon name. The "View Active Clients" list on the Access Controller 720wl shows the client logged in under the original user name, but the Access Controller 720wl log records the SSH login from that client under the shared (duplicate) user name. (1708)

- When an Access Controller 720wl reboots, it loses all knowledge of clients logged on prior to the reboot. However, the Rights Manager will still show those clients in its Clients list. Doing a backup and restore of the Access Control Server 740wl or Integrated Access Manager 760wl will remove all dynamic client information, thus clearing any stale client information. (1818)
- On the Rights Manager Clients page, for clients identified by MAC address, if you change a client identified as an Access Point to "Not an AP", that client is removed from the Access Point group, but the MAC address remains in the built-in database as an Access Point type user, and will not be required to authenticate. If this is a client that should be authenticated (for example, a regular laptop user that you accidently set as an Access Point) you must go to the Users page in the Rights Manager and delete the MAC address from the built-in database, so that the client will be required to authenticate. (2371)

How to get help

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