ProCurve Networking
HP Innovation

The ProCurve Secure Access 700wl Series Version 4.5.0.41 Release Notes

Contents

Software Version: 4.5.0.41

Part Number: 5990-5989
Date: February 2007

Go to the support web site located at http://www.procurve.com for the latest information on the ProCurve Secure Access 700wl Series products. The current release notes, manuals, FAQs, and problem reports are always available at this site.

Important information required for updating system software is available on a secure page at the ProCurve Networking web site: http://www.procurve.com. Click on **Software updates** (in the sidebar). Under **Latest software**, 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.

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

NEW FEATURES IN THIS RELEASE

Following are the major new features of the HP ProCurve Secure Access 700wl Series 4.5.0.41 software.

- Daylight Savings Time update to conform to the U.S. Energy Policy Act of 2007.

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.procurve.com 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 4.5.0.xx the following client browsers have been fully tested and are supported for use with the Administrative Interface:

Operating System	**Browser Software**
Windows 2000 or XP	Internet Explorer 6.0 Netscape 7.1 Firefox 1.0 Mozilla 1.7.5
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. (19024)

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

UPGRADE NOTES

Important: Please read the *ProCurve Secure Access 700wl Series Software Version 4.5.0.xx Update Guide* for instructions on updating your systems that currently run software version 4.1.3.93. The Update Guide applies equally to this patch release.

The update process is a two-step process, requiring an intermediate update to software version 4.1.4.8 before updating to 4.5.0.xx. If you do not update through the intermediate version, you will not be able to downgrade back to the 4.1.3.93 software should the need arise.

If you are running a 4.4 version, you can perform an upgrade directly to 4.5.0.xx.

The *ProCurve Secure Access 700wl Series Software Version 4.5.0.xx Update Guide* may be downloaded in PDF format from the HP ProCurve Technical Support web site at http://www.procurve.com.

Important: Back up your systems before upgrading to the version 4.5 software!

CLARIFICATIONS AND USAGE NOTES

- This release includes a Daylight Savings Time update to conform to the U.S. Energy Policy Act of 2005.
- VLAN Enhancements. The ProCurve Access Controller 700wl Series now provides native
- Cross-VLAN functionality has changed in the ProCurve Software Release 4.5.0.xx. For client cross-VLAN communications, traffic from clients on different VLANs is no longer directly switched between VLANs within the ProCurve module. Instead, all cross-VLAN traffic is forwarded to the Uplink networks for traffic forwarding. Properly configured networks on the Uplink should be designed to handle this function, as this is the only way to ensure that all cross-VLAN traffic is verified as part of the organization's access policies.
- The Integrated Access Manager 760wl no longer supports remote Access Controllers, the ProCurve Access Controller 720wl (J8153A) or the ProCurve Switch xl Access Controller Module (J8162A) A 760wl can only be used as a stand-alone unit.
- Release 4.1 on an Access Controller will not work with release 4.4 on an Access Control Server.
- After migrating to version 4.5.0.xx, a downgrade can only be made to version 4.1.4.8. If the alternate version is lower, 4.1.4.8 must be obtained to ensure a proper downgrade. For more information, see "Downgrading to the Previous Release" in the *ProCurve Secure Access 700wl Series Software Version 4.5.0.xx Update Guide*.
- Network and subnet configuration data is split between local network information and global network information. Configuration data that is likely to be shared between different Access Controllers is stored in global subnet groups. This includes information like DNS, WINS and domain names. These fields are entered manually or can be automatically set from information in a DHCP lease.

If a global subnet group used by a local subnet on an Access Controller is deleted, the configuration information is lost. The subnet group may be automatically created as a placeholder, but the DNS, WINS and other settings must either be manually set or regenerated via a DHCP lease renewal. If the information can be obtained through DHCP, then the information may be renewed by deleting a related local subnet, waiting about 10-15 seconds and then re-entering the local subnet configuration for the subnet. The lease should be renewed and the information in the lease renewal will be used to recreate the global subnet group.

- The failover functionality of the built-in RADIUS server when in proxy mode is as follows:
  - When the first remote RADIUS server is found to be down, an Access-Reject is sent to the client and the proxy server marks the remote server as dead. If the client retries during the dead time (by default—two minutes), the request is sent to the alternate remote server.

  The end user experience is that the first authentication fails if the primary remote server is dead and the second attempt, if made within the two minute timeframe, will succeed.
- Clock synchronization intervals are as follows:
  - External NTP server—30 minutes
  - Internal NTP server between redundant Access Control Servers—25 minutes
  - Internal NTP server between Access Control Server and Access Controller—8 minutes (19724)
- 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 Interface 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. For further information please refer to the Microsoft knowledge base article *Troubleshooting Windows Firewall settings in Windows XP Service Pack 2* at http://support.microsoft.com/default.aspx?kbid=875357. (19360)
- 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. (18987)
- 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. (19336)
- After changing the time zone on a 700wl Series system unit, it takes approximately seven seconds for the new time to take effect. (19355)
- 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. (19359)

- 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 Interface) 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. (18719)
- 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. (18750)
- 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. (18829)
  - 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. (18830)
  - Multicast streams such as IPTV and VPN tunneling (IPSec, L2TP, or PPTP) are incompatible. Multicasting will not work for clients using VPN tunneling. (18832)
- 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 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 ProCurve Secure Access 700wl Series product to your NTP server.
- 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 when roaming with PPTP or L2TP.
- 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 error messages in the logs. These errors are identified 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 an Odyssey is a wireless LAN client or Windows XP wireless 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. (19782)
- 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. (17040)
- If you need to modify the 700wl Series system bridging options through the Advanced Network Configuration page under the Local Networks 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. (17109)
- 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.

SOFTWARE FIXES

The following problems that were identified in previous releases of the ProCurve Secure Access 700wl Series system software have been fixed in software release 4.5.0.41:

- •Daylight Savings Time update to conform to the U.S. Energy Policy Act of 2007.

The following problems that were identified in previous releases of the ProCurve Secure Access 700wl Series system software have been fixed in software release 4.5.0.40 (not a general release):

- Out of order fragmented UDP packets were not re-assembled correctly by the 720wl Access Controller or the Access Control Module (ACM), thus causing session timeouts and lose of connectivity for downlink clients.

The following problems that were identified in previous releases of the ProCurve Secure Access 700wl Series system software have been fixed in software release 4.5.0.37:

- When attempting to shut down the 745 via the LCD panel, the system does not shutdown. (23393)
- Upgraded Apache software to version 2.0.52_4 to address a vulnerability on the ACS 745. (#23394)
- Access Controller intermittent disconnects from Access Control Server. (20529, 20945)
- Access Controllers sometimes cannot display any clients after upgrade. As a workaround, modifying a configuration item will usually fix this. (20669)
- Users authenticating with 802.1X Logons and associated with a Connection Profile that specifies a VLAN ID will not get the correct rights row in the Rights Assignment table. (19849)
- A client with a static IP and valid address on the uplink does not always get redirected. (20832)
- An Access Controller IP address is not correctly displayed with CLI “show clients” command. (20753)
- Access Controllers are not displayed in user interface when using Internet Explorer on Windows 2003 Server. (20771)
- Retrieving client or session status may cause an Access Controller to reboot. (20730)
- The first time the 802.1X/WPA page is viewed, an error message is displayed stating that WPA is not configured. To remove the error message, click the “Save” button. (19849)
- After performing a back-up on the Access Control Server, local host events are not logged. Access Controller events are still logged after a back-up. (19801)
- Several minor error messages and minor information messages are added to the log when a client attempts to access a restricted page. (19394)
- In order to perform a Trace Transaction when using Kerberos, the date and time settings must match between the Access Control Server and the Key Distribution Center (KDC). (19908)
- A QoS Marking name may consist of 1 to 32 characters. If the name is one character long, it cannot be the number zero (0). (19872)
- 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@. (19410)
- 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) (18869)

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.

- Cisco Access Point using the Aironet series of protocols when connect downstream of an Access Controller could originate traffic with the same source MAC address on multiple VLANs or VLANs and untagged networks. This may trigger undesirable behavior on the Access Controller causing it to detect the Access Point as roaming between VLANs. The behavior of clients downstream of this Access Point is undefined. In order to avoid this behavior it is recommended that either the Cisco Aironet series of protocols are disabled or that these series of protocols exhibiting this behavior are blocked through traffic filters that may be configured on the AP. (21090)
- Windows XP and 2000 clients in NAT mode may not accept a DHCP lease if a domain name is not defined on the system. (21088)
- An Access Controller may erroneously display an IP address of 42.0.0.2 on the LCD panel. (21055)
- After migrating to version 4.4, a 1000Base-SX port is described as Ethernet as opposed to 1000Base-SX or 1000Base-SX full-duplex. (20918)
- In a redundant Access Control Server configuration an Access Controller may not show a connection to an Access Control Server if the secondary Access Control Server is not reachable. (20578)
- Under certain circumstances the uptime may displayed incorrectly which can be corrected by manually setting the time and a system reboot. (20825)
- If many Kerberos clients continually log in or out through L2TP every 10-15 seconds (approx. 120 authentications per 60 seconds totally), some authentications may fail. The Windows XP clients which fail to authenticate due to system error #691 (i.e. user name/password invalid in domain) will succeed in the subsequent attempts and ping real-IP peer client. (21054)
- If an Access Controller is downgraded from version 4.4 to 4.1, several disklabel warning messages are issued. These errors are harmless and only appear when version 4.1 is started. (20823)
- Exporting the Rights configuration does not export the list of files used in Logon Customizations. (19914)
- If bandwidth limits are modified in an Access Policy used by an encrypted client, and if the encrypted client has completed a roam before the bandwidth limits were changed, the new bandwidth limits will be displayed correctly in the Client Details page when the “Refresh User Rights Now” is selected. However, the bandwidth limit changes will not take affect until the encrypted client logs off and logs on again. If the encrypted client does not roam during the bandwidth limit changes, the changes take affect immediately after the “Refresh User Rights Now” is selected. (19910)
- In the 802.1X/WPA authentication service with the built-in RADIUS server configured as a proxy, if a client keeps getting authentication failures, verify the following:

  - All components of the authentication service (access points, remote RADIUS servers, clients) are EAP-compatible.
  - 802.1X/WPA authentication service is configured correctly within the 700wl Series system and for each component (access point, remote RADIUS server, and client). For instance:
    - Shared secret and IP address of the remote RADIUS server is correct
    - Access Control Server is a client on the remote RADIUS server configuration

  If all of the above is correct and the client still cannot authenticate, restart the built-in RADIUS server by rebooting the Access Control Server, or contact ProCurve Technical Support for assistance. (19884)

- QoS classification cannot be performed on encrypted (L2TP, PPTP, IPSec) client data. Encrypted data paths consist of inner and outer tunnels, where the outer tunnel is the encryption tunnel and the inner tunnel contains the data packets. QoS classification is currently performed on the outer tunnel. (19871)
- In a redundant system, if there is loss of connectivity between the preferred primary Access Control Server and the secondary Access Control Server, the secondary will promote itself to acting primary. If clients log on to an Access Controller connected to the new acting primary Access Control Server and then connectivity is restored between the preferred primary and secondary Access Control Servers, the restored preferred primary Access Control Server may have a different view of the network than actually exists. This could result in inaccurate information being displayed in the Client Status page. Note that clients do not experience a disruption of service and clients will reappear in the Client Status page once their rights expire or when they logout and log back in. (19808, 19677)
- In a redundant system, 802.1X/WPA Authentication Service configuration is sometimes not replicated on the secondary Access Control Server when redundancy is enabled after the 802.1X/WPA Authentication Service is configured. The workaround is to enable redundancy and let the Access Control Servers peer up before configuring the 802.1X/WPA Authentication Service. (19793)
- In a redundant system, if the secondary Access Control Server is disconnected from the network, an Access Controller will maintain connectivity to the preferred primary Access Control Server and will remove the secondary Access Control Server's IP address from its configuration under the assumption that redundancy has been disabled. The Access Controller will not know about the secondary Access Control Server unless the preferred primary Access Control Server is shutdown, at which point the preferred primary Access Control Server will send a message telling the Access Controller to try to connect to the secondary Access Control Server and will include the IP address of the secondary Access Control Server.
- If the preferred primary Access Control Server is disconnected from the network, the Access Controller connects to the secondary Access Control Server and keeps trying to connect to the preferred primary until eventually after several unsuccessful attempts to connect, the Access Controller removes the preferred primary IP address from its configuration under the assumption that redundancy has been disabled. (19758)
- When the Access Control Server is configured to use the internal Access Controller's HTTP proxy server, clients will not be able to access web sites that use HTTPS. (19749)
- Clients using a Real IP 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. (19427)

- 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. (19354)
- The "Maximum Concurrent Logons per User" setting in an Access Policy does not apply to sessions using SSH port forwarding. (16236)
- 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). (17472)
- 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. (17813)
- 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 Interface 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. (18819)
- Access Control Server may display Access Controller logs with an incorrect timestamp after a reboot of the Access Controller. (20824)
- "Reset to Defaults" button in the Administrator SSL page may not be working. (20657)
- RealIP IPSec client traffic is redirected to the default router even if staying on the local network. (20760)
- Some PPP clients may be denied login (with error message) under heavy PPP system load. (20749)

How To Get Help

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