Release Notes: ProCurve Management Software

ProCurve Manager Plus Version 2.2.1

Mobility Manager Version 1.1

Identity Driven Manager Version 2.15

Network Immunity Manager Version 1.0

IMPORTANT: This release is for new installs and upgrading from PCM 2.1 or earler. Use PCM 2.2 Update 1 to bring PCM 2.2 installations up to the fix level of PCM 2.2.1.

The following products are included and available for purchase in this release.

ProCurve Manager Plus. ProCurve Manager Plus 2.2 (PCM+) is licensed by number of network devices (switches and access points) managed. There are three levels of license:

- J9057A ProCurve Manager Plus 2.2, 50-device base license
- J9058A ProCurve Manager Plus 2.2, +100-device license
- J9059A ProCurve Manager Plus 2.2, unlimited-device license

NOTE: Licenses for PCM+ 2.0 and PCM+ 2.1work for PCM 2.2.

- To upgrade from PCM 1.6 to the PCM 2.2 you must purchase the appropriate licenses, as indicated below.
  - For networks from 50 to 250 managed devices, use a combination of 50 device license (J9057A) and 100 device licenses (J9058A) to match the number of devices in your network.
  - For Networks with more than 250 devices, use the unlimited license (J9059A).

ProCurve Mobility Manager. ProCurve Mobility Manager 1.1 (PMM 1.1) is a plug-in module to PCM+ 2.2 that provides additional management capabilities for ProCurve wireless access points. Licenses for PMM 1.0 will work for PMM 1.1.

- J8990 ProCurve Mobility Module 1.1

ProCurve Identity Driven Manager 2.15. ProCurve Identity Driven Manager 2.15 (IDM 2.15) is a fee-based upgrade to IDM 1.0. For IDM 2.15, there are two levels of license, based on the number of managed users. The base product license is for 500 users, and you can purchase additional 2000-user licenses as needed to manage large user environments.

- J9012A ProCurve Identity Driven Manager 2.15 base product - 500-user license
- J9013A ProCurve Identity Driven Manager 2.15 base product - upgrade from IDM 1.x to IDM 2.15, 500-user license
- J9014A ProCurve Identity Driven Manager 2.15 additional 2000-user license

Network Immunity Manager. ProCurve Network Immunity Manager is a plug-in module to PCM+ 2.2 that can detect and respond to virus attacks on per port basis.Together with (PCM+), Network Immunity Manager provides an affordable, feature-rich, unified, centralized approach to network security management

- J9060A ProCurve Network Immunity Manager 1.0 50-device base license
- J9061A ProCurve Network Immunity Manager 1.0 +100-device license
- J9062A ProCurve Network Immunity Manager 1.0 unlimited-device license

Free Trial Versions

This compressed, ZIP-format file contains a 30-day free trial of these three products:

- ProCurve Manager Plus version 2.2.1,
- ProCurve Mobility Manager version 1.1,
- ProCurve Identity Driven Manager version 2.15, and
- ProCurve Network Immunity Manager version 1.0

These release notes include information on the following:

- New Features
- Installation Requirements
- Installation Notes
- One Network Management Program per Computer
- Working With Multi-homed Systems
- Adding Remote Client Stations
- Configuring Client/Server Access Permissions
- Receiving Traps Using ProCurve Manager
- Support for ProCurve Wireless Devices
- Support for ProCurve 9300 Series Devices
- ProCurve Mobility Manager 1.1 Notes
- ProCurve Network Immunity Manager 1.0 Notes
- Other Known Issues

NOTE: These Release Notes are applicable at the date of the ProCurve Manager Version 2.2.1 Release. Please check the ProCurve Technical Support Web site at www.procurve.com for more recent information.

New Features

Below is a summary of the new features that are available in ProCurve Manager Plus (PCM+) with this release. This release contains the same new features as ProCurve Manager Plus 2.2. Please refer to the ProCurve Manager 2.2 Network Administrator's Guide for a full description on the use of these features:

ProCurve Manager Plus v2.2/2.2.1 Features:

Policy Management. Create proactive policies that will enable immediate network action without intervention. Revamped interface that lets you define event-driven and scheduled Policies, with separately defined actions that can be applied automatically in response to an event alert.

MAC Lockout. Blocks a specific MAC address so that the switch drops all traffic to or from the specified addresses.

Virus Throttling. Modify and view VT configuration parameters along with creating and deploying VT policies

Port Mirroring. You can now use PCM+ to configure port mirroring for network monitoring. On select ProCurve devices you can configure Remote Port Mirroring to forward traffic to another device for additional analysis.

Added SNMPv3 Support. PCM now supports SNMPv3 trap decoding. That is, PCM can be a trap receiver for devices that are configured to send v3 traps.

SCP and SSH Support. With PCM 2.2, implementation of SCP (Secure Copy) provides a secure alternative to TFTP for transferring sensitive switch configuration files to and from the switch. SCP is an implementation of the BSD rcp (Berkeley UNIX remote copy) command tunneled through an SSH connection. SCP works with both SSH v1 and SSH v2.

Configuration Import and Export. New configuration import/export feature lets you save device configuration to .csv file, and import device configuration files in the same format.

Enhanced Discovery. Responsible for discovering and determining the topologies of devices in the network. Improved algorithms to speed up the discovery process.

Enhanced Event Filtering. Quickly find specific notifications by sorting & filtering.

Revamped Custom Groups. Custom Groups now allow a hierarchy of folders and subfolders so you can create a group that matches to your locations. In addition, group membership can be defined to port granularity, allowing a single device to span multiple groups.

Traffic Monitoring. Traffic monitoring is now set to run automatically, with the capability for simultaneously performing statistics polling and sFlow (or XRMON) sampling, on both ingress and egress traffic. Improved sampling algorithms reduce traffic monitoring overhead and improve traffic performance.

Device Access and Port tabs. New Device Access and Port List tabs provide additional details on device security settings and port access configurations.

Network Maps. Improved Network Map displays, include additional details on link status, VLAN connections, and Traffic between devices. You can also add background images, and save a specific network view as the default map display.

Audit Logging and Reports. To support the increasing need for IT audit and reporting, PCM provides an audit log function to track configuration changes. Five new security reports provide information on device security settings, password policy compliance, and security history to assist in meeting regulatory compliance for security.

Mobility Manager 1.1 Features:

ProCurve Mobility Manager (PMM) is a simple yet powerful management tool to centrally configure, update, monitor and troubleshoot a ProCurve wireless LAN. Mobility Manager extends the capabilities of ProCurve Manager Plus, with functions specific to the management of wireless APs, including radio properties and configuration of WLANs.

New features in PMM 1.1 include support for the ProCurve WESMxl and radio port products. In addition, significant enhancements have been in the interface. PMM 1.1 has improved, easier to use navigation, wireless and radio information tab displays, and tools to configure and deploy WLANs.

With Mobility Manager you can perform commonly used operations on multiple radios simultaneously, such as setting the channel, transmission power, RF detection parameters, and radio state.

Mobility Manager lets you review and revise security related information in “WLAN security configurations”. These include SSID, VLAN, closed system, encryption, authentication, and key management for static WEP, WPA-PSK, and RADIUS authentication servers.

Identity Driven Manager 2.15 Features:

With IDM 2.15 you get an update to the underlying datastore and events display, to take advantage of the improvements made in the PCM 2.2 application.

You can now use IDM with any of the following RADIUS servers: Microsoft IAS, Funk’s Steel-Belted RADIUS (SBR), and freeRADIUS on the following Linux platforms; RedHat 3, and 4 (Enterprise Edition), SuSe 9.3 Enterprise Edition, and SuSe 10 Desktop Edition.

Network Immunity Manager 1.0 Features

The Network Immunity Manager is a plug in to PCM+ and allows security policy setting and monitors virus activity on the network. NI Manager detects viruses by behavior anomaly detection on sampled traffic and it accepts virus detection alerts from switches running Virus Throttle software, and from IDS/IPS/UTM security appliances.

The Network Immunity Manager detects zero day attacks (first attacks by a new virus) and protects against threats from inside the network such as an employee bringing an infected laptop in to work. Fast automated response to virus attacks by taking action on the source port of the attack is how NI achieves protection.

Installation Requirements

Supported Software

ProCurve Management software is supported on the following Operating Systems:

- MS Windows 2003 Server
- MS Windows XP Pro (Service Pack 2 or better)
- MS Windows 2000 (Server, Advanced Server, or Pro with Service Pack 4 or better)

ProCurve Manager software is not currently supported on Vista.

System Requirements

Network size/ Install type	CPU	RAM	Free Disk Space	NIC
Small-Medium/Min.	2 Ghz Pentium IV*	1 GB	10 GB	1 GB NIC
Small-Medium/Max.	3 Ghz Pentium IV*	2 GB	40 GB	1 GB NIC
Medium-Large/Min.	3 Ghz Pentium IV*	2 GB	40 GB	1 GB NIC
Medium-Large/Max.	Intel Xeon	4 GB	80 GB	1 GB NIC

* Intel Pentium IV or equivalent processor

- Small - Medium, Minimum = one 50-device starter license (J9057A), installing only PCM/ PCM+ on network with 50-250 managed devices
- Small - Medium, Maximum = one 50-device starter license (J9057A) and two 100-device incremental licenses (2 each, J9058A), installing PCM+, IDM, PMM, and NI products.
- Medium-Large, Minimum = 50-device starter license (J9057A) and two 100-device incremental licenses (2 each, J9058A), installing only PCM/PCM+
- Medium-Large, Maximum = an Unlimited license (J9059A), installing PCM+, IDM, PMM and NI products.

ProCurve Manager for OV-NT Network Node Manager Requirements

- ProCurve Management software is supported on HP OpenView Network Node Manager for Windows, versions 6.4, 6.41, 7.01, or 7.5.

ProCurve Identity Driven Manager (IDM) Requirements

- Use of the IDM software requires implementation of one of the following access control methods: MAC-auth, Web-auth, an 802.1x supplicant application, or RADIUS.
- The following RADIUS versions are supported: Microsoft IAS, Funk's Steel-Belted RADIUS (SBR), and freeRADIUS on the following Linux platforms; RedHat 3, and 4 (Enterprise Edition), SuSe 9.3 Enterprise Edition, and SuSe 10 Desktop Edition.
- For assistance with implementation of RADIUS and access control on your network, contact the ProCurve Elite Partner nearest you that can provide ProCurve Access Control Security solutions. You can find ProCurve Direct Elite partners on the web at:
- http://hp.via.infonow.net/locator/us_partner/index.jsp

Installation Notes - General

The installation download for PCM 2.2.1 contains PMM 1.1, IDM 2.15, and NIM 1.0 installation files.

- If you are running PMM 1.0, you must select the PMM option during the PCM 2.2/2.2.1 install process. This will install the GUI and database updates for MM1.1.
- If you are running IDM 1.0 or 1.0.x, you must select the IDM option during the PCM 2.2/2.2.1 install process. This is required to support changes made in the underlying PCM and IDM databases. If you have not purchased an IDM 2.0 or newer license, your installation will include the IDM interface changes made for IDM 2.0 and IDM 2.1, but all new functionality (FUNK SBR support, User Import/Export, Access Control, and Endpoint integrity support) will be disabled until you purchase and register an IDM 2.1 license.
- If you want to test the IDM 2.15 functionality using the free 30-day trial provided with PCM 2.2/2.2.1, you need to install the software on a separate system that has no previous IDM version installed or in use. Once you upgrade to PCM or PCM+ Version 2.2 or newer and IDM 2.15, you can not revert to the previously installed version. If you are uncertain if you want to upgrade to the 2.2/2.2.1 Version, it is best to install it on a system that does not have any earlier versions of PCM or IDM installed.

If you are upgrading from ProCurve Manager 1.6, back up the \PNM\server\db\solid.db database file before beginning the installation wizard. This will allow you to restore your data in the event that the existing database gets lost or corrupted during database migration

If you are upgrading from ProCurve Manager 2.x, back up the \PNM\server\mysql directory before beginning the installation wizard. This will allow you to restore your data in the event that the existing database gets lost or corrupted during database migration.

When the PCM installation starts to copy files to your system, do not cancel out of the installation. Please finish the installation, and then run the uninstall via "add/remove programs" in the Windows control panel to remove the installed files. If you do cancel out, you may not be able to uninstall.

ProCurve Management software is not localized for non-English versions of Windows.

One Network Management Program per Computer

Make sure you uninstall any other network management programs from your computer before installing ProCurve Manager or ProCurve Manager Plus, because a resource conflict will occur if you have multiple network management tools running on the same computer, for example during discovery of the network devices.

Note: The above is not applicable when PCM 2.2.1 is installed on systems running HP Openview NNM.

Working With Multi-homed Systems:

A multi-homed system is a server or PC that has more than one IP address. Generally this is achieved by installing more than one network card in the system, but there are other ways that a system can be multi-homed. Here are a few of the situations that meet this definition:

- A system with two or more network adaptors.
- A system with a traditional ethernet network adaptor, plus a wireless adaptor.
- A system with only one network adaptor, but that is running some network tunneling software such as a VPN client. Generally what happens in this situation, is that the system appears to have two network interfaces (each with its own IP address). But in reality the system only has one physical adaptor, and the VPN client software emulates a second adaptor (while using the original adaptor under the covers).

When ProCurve Manager (either client or server) starts up, it attaches itself to the primary network interface. All network traffic between the client and server will be directed to the selected network interface. For example, if the ProCurve Manager client application attaches itself to the 192.3.4.5 interface, and the ProCurve Manager server is running on the 10.255.120.* network, there is no way that the client will ever connect successfully to the server.

To resolve this problem PCM has a configuration file that you can change to correct this situation. To setup this file, follow these steps:

1. Find the commIpAddr.txt file. This file exists in the config directory, so for example, for the client this file exists in: C:\Program Files\Hewlett-Packard\PNM\client\ config. For the PCM server, you need to create a text file (with Notepad or similar application) and name it "commIpAddr.txt" and place it in the C:\Program Files\Hewlett-Packard\PNM\server\config directory.
2. Edit the file with a text-based editor (such as Notepad or WordPad), and enter the IP address of the interface you want the application to attach to. For example for the network illustrated above, you would add the entry " 10.255.120.25 " (without the quotes) in the first line of the file. More than one IP address can be used, but each IP Address entry must be on a separate line.
3. Save your changes.
4. Restart the application. If this is the ProCurve Manager client, just restart the application. If this is the ProCurve Manager server, you must restart the PCM services (HP ProCurve -Datastore, -Network Manager Server, and -Traffic Launch Service) from the Services control panel.

Adding Remote Client Stations

When you install ProCurve Manager Plus, the server and client functions are installed on the computer. You can also install the client function on any number of other computers in your network that have network access to the server computer.

To install the client function on another computer, simply start a Web browser, such as Microsoft Internet Explorer, and for the URL type in the IP address of the server computer followed by a colon and the port ID 8040. For example, if the IP address of the server computer is 10.10.20.25, then you would enter "http://10.10.20.25:8040" on the Web browser address line. That will launch the client installation wizard and step you through the installation process.

If you have multiple ProCurve Manager servers in the network, when you install a remote client you will be prompted to select the server to which you want the client to attach. This server will be used each time the client program is launched. You can change the server that is being accessed by selecting the "ProCurve Manager Server Discovery" option that was included when you installed the client. From the Windows "Start" menu, select Programs ->ProCurve Manager ->ProCurve Manager Server Discovery

For the PCM-NNM version, the PCM Remote Client can only be installed on machines that have the NNM Remote console installed. Once installed, the client will always connect to the server attached to the NNM remote console.

If a PCM remote client attempts to connect to a PCM server, and that server has a firewall turned on, the PCM remote client will come up with the message "no context defined" and a grey (empty) display. The firewall prevents the PCM remote client from getting the necessary connection and data files from the PCM server. You must disable the firewall on the PCM server, or configure the firewall to allow the PCM remote client and PCM server to communicate.

Configuring Client/Server Access Permissions

The ProCurve Manager server maintains a list of authorized clients that are permitted to log into the server. By default, when the ProCurve Manager server is installed, the only client allowed to log in is the client on the same system as the server--that is, no remote servers are allowed. This can be a problem for customers who are unaware of this security feature, because they will try to install remote clients using the browser, and will be unable to connect to the server after completing the client installation.

There are two files associated with ProCurve Manager client/server security that can easily be configured to allow access to any set of actual or potential clients. There are two ways that this file can be configured, depending on what you know about the clients that need to connect.

IP addresses. The access.txt file can be configured with a list of IP addresses specifying the clients that are authorized to log into the server. The file may contain as many addresses as needed, one IP address per line; or you may configure IP addresses with wildcards. DNS names are also allowed in the file, including DNS names with wildcards (this is useful for DHCP environments where a system's DNS name remains unchanged, although it's actual IP address may change from time to time). For example, below is an example of a valid access.txt file:

```
10.255.124.84
10.29.37.*
10.*.*.*
*.rose.hp.com
system1.hp.com
```

To add an entry, open the access.txt file, which can be found in the config directory (C:\Program Files\Hewlett-Packard\PNM\server\ ). Be sure to edit the file using a text-based editor such as Notepad or Wordpad. Edit the file as necessary, one entry per line, then save it. It is NOT necessary to restart the server; the changes will take effect immediately.

Passwords . There are situations where it is not possible to know ahead of time what IP address a potential client will have. This is particularly the case in situations where the client comes in through a VPN, where the IP address of the client is assigned externally. To solve this problem it is possible to add client passwords to the access.txt file that correspond to specially configured clients. Note that even though you will be modifying the same access.txt file as for method 1 (above), the two mechanisms can freely co-exist--that is, the access.txt file can contain a combination of IP addresses and passwords. To enable password access for a particular client, follow these instructions:

1. First you must change an entry in the server\config\TyphoonServer.cfg file.

   This file is a text file and can be edited with Notepad or Wordpad. Look for the entry that reads "`AUTHENTICATION=10`", and change it to read " `AUTHENTICATION=100` ".

2. Save the file and restart the server (listed as "HP ProCurve Network Manager Server" in the services list).

3. Edit the access.txt file as described above, but instead of entering an IP just enter the selected password (on a line by itself). Save the file. It is not necessary to restart the server. For example, if we set the password to "procurve":

   ```
   procurve
   *.rose.hp.com
   system1.hp.com
   ```

4. On the client (the client must already be installed), you must edit the riptide.cfg file. This file already has several entries in it. You must add a line similar to the following:

   ```
   PASSWORD = user_password
   ```

   where user_password is the password the client will use to access the server.

   Do not change any of the other entries in the file, as they are necessary for the correct operation of the client.

   A sample Riptide.cfg file, once edited with the password "procurve", would look like this:

   ```
   LEASE_LENGTH = 40000
   TRACING_PROPERTY_KEY = CoreServices.Main
   MANUFACTURER = Hewlett-Packard
   SERVICE_NAME = Typhoon
   COMPONENT_DB = config/Components.prp
   TRACING_DBFILE = config/Loggers.prp
   NETWORK_DELAY = 25000
   VERBOSE = true
   PASSWORD = procurve
   ```

5. Once you have saved the riptide.cfg file, start the PCM Client and enter (select) the address of the PCM Server in the Direct address field of the "Search for Servers" dialog. The client should now connect successfully to the server.

Note:

If a PCM remote client attempts to connect to a PCM server, and the PCM server has a firewall turned on, it is possible that the PCM remote client will come up with the message “no contexts defined” and a grey (empty) display. The firewall prevents the PCM remote client from getting the necessary connection and data files from the PCM server.

You must disable the firewall on the server, or configure the firewall to allow the PCM remote client to connect to the PCM server.

Receiving Traps Using ProCurve Manager

A trap is an SNMP alert sent by a host device via UDP protocol to notify one or more hosts that something has occurred. A device may send a trap when a link on a port comes up, when a device has received an excessive amount of errors, or when a device has detected an excessive amount of broadcasts. In order to receive traps from a particular device, the switch must be configured with the host's address. This is accomplished in multiple ways, such as CLI, SNMP, and ProCurve Manager.

When ProCurve Manager (server) starts up, it binds to port number 162. Port 162 is the port that all incoming traps arrive on. A problem arises when a previous process is already bound to that port, in which case ProCurve Manager will not be able to receive traps because the port is in use.

To resolve the problem, make sure no process is bound to port 162. Examples of applications that bind to port 162 are the Windows SNMP Trap Receiver Service*, TopTools, HP OpenView and MG-Soft MIB Browser Trap Ringer. In the event that a process was bound to port 162 when ProCurve Manager was started simply terminate the process and restart the ProCurve Manger (server). To restart the ProCurve Manager (server) in Windows 2000 go to Control Panel->Administrative Tools-> Services. Double click on the HP ProCurve Network Manager Server, click the Stop button, and then click the Start button.

In Windows XP/2003 server, go to Control Panel->Administrative Tools-> Services, double click on the HP ProCurve Network Manager Server, click the Stop button, and then click the Start button.

NOTE for PCM-NNM Users:

The above is not applicable for the PCM-NNM installation. PCM cannot bind to port 162 since it is already used by NNM. All device traps and application events will be displayed on the NNM Alarm browser.

Support for ProCurve Wireless Devices

- For the ProCurve Wireless Access Point 420 devices, the PCM Switch Software Update utility will only work with switch software versions newer than 2.0.29
- For the ProCurve Wireless Access Point 520wl devices, if you upgrade to version 2.4.5 of the software, the PCM Switch Software Upgrade utility will not allow you to "downgrade" to an earlier version of the software.
- If you use a 520wl device as the starting point for a managed subnet, Discovery will not work properly unless you manually add the subnet in PCM and then restart Discovery.

Support for ProCurve 9300 & 9400 Series Devices

The following are known issues when using PCM 2.2.1 with the ProCurve 9300 Series devices:

- Port based Policies cannot target a range of ports (e.g., A1-A5, etc.) on 93xx devices.
- LLDP-capable devices connected directly to 93xx devices may not map properly. Using a CDP-capable device between the 93xx and LLDP-capable device will resolve the problem.
- Support of SNMPv3 and SSH Keys on 9300 series devices is not included with PCM 2.1
- VLAN discovery will work for ProCurve 9400 devices; however, the VLAN Manager configuration features are disabled.
- On the 9400s the sFlow SNMP MIB is only visible when sFlow has been previously enabled via the device console. To ease the burden on the user, PCM will attempt to enable the MIB during discovery using the configured CLI login parameters. If these are not correctly configured, the 9400 will not be discovered as an sFlow-capable device; this is evident when attempting to configure the device for traffic monitoring as the Sampler column of the Traffic Device Configuration screen contains "N/A". If this situation arises and the user wishes to collect sFlow sampled data using PCM, the following steps are required.

  a. The 9400 device must be deleted from PCM.

  b. The user must either manually enable sFlow on the device using its console or must correctly configure the device's CLI parameters in PCM.

  c. The 9400 must be manually rediscovered from PCM. It should now appear as a device on which sampling can be enabled.

PCM 2.2.1 Help>About Information

Selecting “About” from the PCM 2.2.1 Help menu displays the same information as PCM 2.2. If PCM 2.2.1 is installed, the following registry entry is present:

HKEY_LOCAL_MACHINE\SOFTWARE\HP\ProCurve Manager\PCMPatchVersion = 2.2.1

If PCM 2.2 is installed, the above registry entry is not present.

Mobility Manager 1.1 Notes

- If the network contains access points that are not configured with the default CLI passwords used by PCM then the elements associated with those access points (e.g., radios, SSIDS) may not be discovered. The user should either pre-configure the devices with the access credentials used by PCM prior to starting discovery or wait until the device is discovered and use the “Communication Parameters in PCM” wizard to override the global defaults. You can then use Manual Discovery to re-discover the device, and its related radios and SSIDs, or you can simply wait until the next regularly scheduled discovery cycle collects the information.
- PR_1000407647 and PR_1000413912 — Caching problems can affect the display of changes for radio configuration parameters.
- PR_1000410783 — When using Manual Discovery for an AP530, if you select the Radios tab before the data has populated, you will see the tab update but no row is highlighted and details are not displayed until you select a row in the tab display.
- PR_1000409277 — When you use “Halt” during processing of multiple WLAN or wireless device configurations, you cannot get a Status Summary for items already processed.
- PR_1000415126 — When a WLAN is first enabled, the details for that WLAN configuration will not appear in the WLANs tab until the next Discovery cycle.
- PR_1000410832 — When using PMM 1.1 to configure a WLAN for AP520 devices, you must use the ‘reboot 0” command on the 520 device before the configuration will take affect.
- PR_1000415723 — When using the “Deploy WLAN Configuration” function for WESM devices, there are only three possible configurations for the Security Suite: WPA Pre-shared Key. Although it appears you can select any combination of Cipher and Version, only the following configurations will be applied:
  - Cipher = CCMP (AES), or TKIP + CCMP (AES), then Version = WPA2
  - Cipher = TKIP, then Version = WPA + WPA2
- PR_1000415730 and PR_1000414850 — On the WESM radios, to perform any RF Detection operation, set System-wide RF Detection State = ENABLE.
  - To disable all RF Detection from the WESM, set System-wide RF Detection State = DISABLE
  - To set a radio to Dedicated multi-channel RF Detection:
    Set System-wide RF Detection State = ENABLE, and Detection Mode = DEDICATED
  - To set a radio to Single channel, passive RF Detection:
    Set System-wide RF Detection State = ENABLE and Detection Mode = NORMAL

  For a WESM using WS.02.XX version software, to set a radio to Single channel, passive RF Detection you must use the WESM devices' Web GUI: Select: Network Setup--> Radio –> Select "Single-channel scan for Unapproved AP's" check box. Click OK, and then Save.

Reference Identity Driven Manager 2.15 Notes

- If you are upgrading from previous versions to IDM 2.15, you must also upgrade the IDM agent. On your system with the RADIUS server, download the latest IDM agent install.exe via http://<hostname of IDM server>:8040. Run this install.exe to upgrade to the IDM 2.15 agent. See the "Getting Started Guide" for additional details.
- When upgrading from IDM 1.0 to IDM 2.0 or newer, if there are users logged in prior to the upgrade the users will appear as logged in after the upgrade. This is not necessarily a problem but, the users will never be shown as logged out even after they logout. There are two possible fixes for this, one is to make sure all users are logged out before the customer performs the upgrade. The other is to reset session accounting statistics after the upgrade has completed, this is done by navigating to Preferences -> Identity Management and clicking on the "Reset accounting statistics" link.
- When upgrading from IDM 1.0 to IDM 2.0 or newer, all previous user session histories will be discarded.
- Depending on the number of users in your environment, IDM performance may be degraded due to large number of events logged during peak usage hours. Symptoms of this include:
  - The login bar chart not reflecting the current number of logins for a given hour,
  - The users' last login time not reflecting the correct time, and
  - More than the maximum allowed number of events in the IDM and PCM event browser.

  You can improve IDM performance in either of the following ways:
  - Turn off "Session Start/Stop events" in the Preferences for Identity Manager, or
  - By setting the "events to ignore: Link up and Link down" options in the Preferences for Events (in PCM).
- If you experience problems with the Logins/Hour chart in the GUI after Daylight Savings Time, you can restart the PCM/IDM server and GUI to work around the problem
- IDM now allows you to configure all 'default' attributes for users that have not yet been configured in IDM to belong to a specific Access Policy Group. In IDM 1.0, you could only set the "default VLAN". In IDM 2.0 or newer, you use the 'Default Access Policy Group' to set any access rules and rights to be applied to users that do not yet belong to an Access Policy Group.
- If you experience performance issues on the PCM/IDM server, consider turning off the "Session start and stop events" (from the Preferences window under Identity Management). Session accounting will still be active, but fewer events will be logged in the event browser.
- When using the IDM User Import function, even if no user is selected to be removed a warning event is displayed in the IDM event viewer about the users being deleted.
- When requesting reports and session information, there may be some delay as the database is processed to find the matching records. This is normal and a function of the size of the database and the performance of the system on which PCM/IDM is running.

- By default you will receive warning messages when IDM sets attributes (e.g. QoS, or rate-limits, or ACLs) that a specific device does not support (e.g. an older device such as a 2500). If you wish to disable these messages you can do so via the Preferences window under Identity Management.
- By default IDM does not show the Endpoint Integrity State as an input to rules in Access Policy Groups. If you are using Endpoint Integrity, you should enable this setting in the Preferences window under Identity Management

Known Issues for PCM 2.2.1

General

- If you reset the system clock on the system where PCM Server is installed, you must restart the HP ProCurve Network Manager Server in the Services window to restore the database connection. (Settings->Control Panel->Administrative Tools->Services)

Installation

- PCM/PCM+ and Terminal Services are not supported on same server

Discovery

- When adding subnets for Discovery in Global Preferences, there is no verification of IP addresses. If an invalid IP address is used, the subnet will not be discovered.
- If you have a very large network with many subnets, PCM performance can be improved by increasing the discovery interval, and in particular increasing the interval for VLAN discovery.
- If you have a large network, and are using a Configuration Scan Policy while Discovery and Traffic Monitor are running, it may cause the PCM management server to 'hang' or lose its connection to the "Typhoon Server". It is best to use a phased method (use separate policies at staggered intervals to scan by subnets or device group) rather than a single policy. Alternately, you can stop the Discovery and Traffic Monitor processes while the configuration scan is being done.

Network Maps

- Wide Area Network (WAN) links are not supported (displayed) in the PCM network maps.
- Path Trace does not work properly in a meshed environment.
- If the device Display Name preferences are changed, you need to refresh (redraw) the network map in order to view the new device display name.

Event Management

- Series 93xx traps are not automatically received by the PCM Event Browser. The Agent IP address that is embedded in the SNMP PDU is not the IP address from which the device was discovered. To resolve the problem, run the following command from the 93xx CLI:

  ```
  snmp-server trap source ve 200
  ```

- Syslog trims entries after 1000 events based on severity, so it trims the events with the lowest severity first.

Traffic Management

- The link speed from a port is sometimes unavailable, meaning that it is specified in the device's SNMP MIB as 0 (zero). Without link speed PCM cannot present any traffic data as it is unable to compute a utilization value. This causes PCM's traffic gauges to appear blank, without an internal "needle". Depending upon the device, this can happen on Ethernet ports that are not being used and may also happen on the WAN ports of 7000s that are running protocols other than PPP (note that traffic monitoring of PPP over ISDN is unsupported). Traffic monitoring of HDLC and Frame Relay WAN links on the 7000s will be available when a firmware update provides link speed for those protocols.
- A bug in the SNMP library used by the traffic data collector can erroneously cause an SNMP error to be reported by the PCM Events viewer. This condition appears only for devices that cannot be used by PCM anyway because another sFlow-capable management station has already "locked" the sFlow MIB of the device. However, when this condition is encountered it can generate a large number of events in a relatively short time.

VLAN Management

- When deleting VLANs directly on the switch, a full discovery cycle must run before changes are displayed in the PCM user interface.
- Creating VLANs in PCM may take several seconds to take effect on switch. To speed up the process, restart Discovery.
- If you create a VLAN directly on the switch (not using PCM), PCM will discover the VLAN at the next discovery cycle. To speed up the process, restart Discovery.

Configuration Management

- Configuration labels cannot be removed until the configuration is deleted.
- When entering IP addresses for devices in PCM, they are not always verified. If an invalid IP address is entered for a device in PCM, then PCM will be unable to communicate with the device.
- Any change made to a device configuration file will cause the Configuration File change indicator to be displayed, even if it is only to the first line (date and version number) of the file and there are no actual configuration changes.

- When RADIUS authentication for managers is configured on a switch, PCM does not support use of CLI. Only local password authentication and TACACS is supported. If you use RADIUS on a switch, the CLI commands, and CLI "Test Communications Parameters" will not work.

Device Management

- When launching the “Communication Parameters On Device” wizard a communication test is performed. If the device is unreachable, or the CLI and SNMP connections cannot be established then a warning is displayed. The user may continue to use the wizard but some operations may fail as a result of the communication problem. It is recommended that the user run the “Test Communication Parameters” tool and resolve any problems reported.

SSH Support:

- SSH support is not enabled by default for 25xx series switches. To enable SSH support the user should ensure that they have upgraded their 25xx devices to a software version that supports SSH (F.04.08 or newer), and then edit the files PNM\server\config\devconfig\sw25*.oid so that the “isSSH=false” line is changed to “isSSH=true”. Once this is done the PCM server services should be restarted. SSH support should now be enabled on the 25xx devices.

PCM-NNM synchronization component:

- Devices deleted in PCM will not be deleted from NNM.
- Changing subnets from Managed to Unmanaged on PCM will not be reflected in NNM.
- If SNMP community names are changed on NNM, the change will be not be reflected in PCM until after the next SNMP synchronization cycle. To speed up this process use the manual SNMP synchronization process.

Software Fixes in PCM 2.2.1 Release

The following problems are resolved in PCM release 2.2.1

- PR_1000415212 — Problem deploying configurations to AP420 devices running switch software version 2.1.7
- PR_1000407748 — PCM does not identify the Access Controller Module (J8162A) correctly.
- PR_1000372265 — Monitors using a 120 DPI setting results in the PCM pull-down menu controls being truncated.
- PR_1000333901 — Inventory reports not sorted correctly
- PR_1000385172 — Cannot schedule staggered OS updates.
- PR_1000395018 — CLI command sent as user name.

- PR_1000393275 — PCM not correctly ordering device firmware releases with five digits.
- PR_1000309521 — PCM Ignores Proxy Configuration.
- PR_1000379464 — In PCM 2.1 Update 8 Preferences>Configuration Management>Switch Software the "Prefer the latest version" checkbox state has to be changed for the Apply button to be available.
- PR_1000426771 — “Download and Install Automatically” feature of Automatic Update does not work.
- PR_1000437688 — PCM reports “Login failed: No user manager server found” and various AIO failure codes.
- PR_1000436776 — PCM reports “Login failed: No user manager server found” and the upgrade fails (does not affect new installations) due to empty custom groups, null BSSID values, or apostrophes in custom group names or descriptions.
- PR_1000439484 — Blank page in Throttled event (Global:Event:Throttled:Events) from the Global Preferences window after an upgrade to PCM 2.2.

Publication Number
5991-8605
July, 2007

Applicable Products
ProCurve Manager v2.2
ProCurve Manager Plus v2.2
ProCurve Mobility Manager v1.1
ProCurve Identity Driven Manager v2.15
ProCurve Network Immunity Manager v1.0

Trademark Credits
Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Software Credits

SSH on ProCurve Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

http:// www.openssh.com.

SSL on ProCurve Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

http://www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com)

Open Source Software Acknowledgement

PCM and PCM+ uses two unmodified Open Source packages. The full source code and licenses to these packages can be found on the PCM distribution CD in the OpenSourcePackages directory. These packages are:

1) JDesktop Integration Components.
http://javadesktop.org/articles/jdic/index.html

2) JRadiusClient. http://jradius-client.sourceforge.net/

The following applies to both of these packages:

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

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.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.procurve.com