# Release Notes:
# ProCurve Manager Version 2.2/2.2.1, Update 5

PCM version 2.2/2.2.1, Update 5 supports these products:

- J9056A ProCurve Manager Plus 2.2 - upgrade from PCM 1.6 license to PCM Plus 2.2 50-device license
- J9057A ProCurve Manager Plus 2.2 - 50-device license
- J9058A ProCurve Manager Plus 2.2 - +100-device incremental license
- J9059A ProCurve Manager Plus 2.2 - unlimited device license, upgrade from PCM 1.6 100-device license

If you are using a version of PCM or PCM+ earlier than PCM 2.2, you must first upgrade to PCM 2.2.1 before you can apply the fixes included in this update. Although it is not recommended, you can also upgrade to PCM 2.2 and manually install PCM 2.2 Auto Update 5, which upgrades previous versions to a PCM 2.2.1 fix level.

These release notes include information on the following:


- Clarifications and updates to text in existing PCM 2.2 product manuals. (Page 4)
- A listing of enhancements included in the Auto-Update releases. (Page 5)
- A listing of software fixes included in the Auto-Update releases. (Page 7)


### Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at **http://www.procurve.com**. Click on **Technical support**, then **Product manuals**.

- Read Me First for the ProCurve Manager, Version 2.2
- ProCurve Network Management Getting Started Guide
- ProCurve Manager Plus 2.2 Network Administrator's Guide

### Publication Number

5991-8611
September 27, 2007

### Applicable Products

- J9057A ProCurve Manager Plus 2.2 - 50-device license
- J9058A ProCurve Manager Plus 2.2 - +100-device incremental license
- J9059A ProCurve Manager Plus 2.2 - unlimited device license, upgrade from PCM 1.6, 100-device license
- J9056A ProCurve Manager Plus 2.2, upgrade from PCM 1.6 license - 50-device license

### 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)

### 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

# Software Management – ProCurve Manager 2.2/2.2.1 Updates

If you installed PCM 2.2.1, you can install this ProCurve Manager update using the "Automatic Update" feature in PCM+, or you can install it manually. If you installed PCM 2.2 and have not installed an update manually, you must install this update manually.

To verify if the Update has already been installed, look in the Update History window under the PCM Global Preferences:

```
[Tools->Preferences->Automatic Updates->Update History]
```

### Using the PCM Automatic Update to Install

1. Open the Preferences panel in the PCM Client and select the **Automatic Updates** node.
2. Click the **Check Now** button. A dialog appears with a list of the available update(s).
3. Select the update, ensure that the **install** checkbox is enabled and click the **Next** button.
4. A warning message appears, advising you that any PCM clients will be disconnected. Click **OK** to continue.
5. After the update package is downloaded, you will be prompted to close the PCM Client. Click **OK** to close the pop-up, then close the Preferences window and exit PCM.

The update will be applied and the PCM services restarted. Once this is done you can reconnect with the PCM client and begin using the updated version of PCM.

### Using the Manual Process to Install

1. Copy the pcm_2_2_update_5.zip file to the \PNM\server\data\download\autoupdate directory.* (Do not unzip the file.)
2. Open the Preferences panel in the PCM Client and select the **Automatic Updates** node to display the Global:Automatic Updates panel.
3. Click the **Check Now** button at the bottom of the panel to display the **Select update mode:** dialog.
4. Select the **Check for updates in PCM's download folder** option and press **Next**.
5. You should see the new auto-update presented for installation, and you can continue with the Update installation (steps 3 through 5 above).
6. Restart the client and verify that the update was applied by checking the **Update History** node located under the Automatic Updates preference node.

* The default PCM server installation directory is: C:\Program Files\Hewlett-Packard\PNM\server on the workstation where PCM was initially installed.

# Clarifications and Updates

## Update 3

- IPS support for the SonicWALL Pro Series Unified Threat Management (UTM) appliances, version 4.0.0.0-39e of the SonicOS firmware. This support gives PCM and Network Immunity Manager the ability to process IPS SonicWALL traps and take action, as configured by the user. These appliances prevent damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content.

  SonicWALL appliances are automatically discovered by PCM. However, you must configure the following PCM setting for proper operation:

  NOTE: All discovered UTMs, regardless of vendor, are placed in the UTM folder in the PCM navigation tree. Although PCM discovers SonicWALL appliances, they are not included in Network Maps. Instead, they appear in the unmapped devices section.

  - If the UTM is configured with a unique read and write community name (other than PCM's default of "public"), configure the community names in PCM.
  - Configure the switch port connected to the UTM as a member of each VLAN where attacker or victim traffic might originate.

  For additional SonicWALL UTM information, see the forthcoming Network Immunity Manager Implementation Guide (accessible by registering at my.procurve.com).

## Update 2

- Support for FortiGate Unified Threat Management (UTM) appliances from Fortinet (third-party network security appliances), version 3.0 firmware build 480 of the FortiOS firmware. This allows PCM and Network Immunity Manager to process IDS and IPS Fortinet traps and take action configured by the user. These appliances prevent damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content.

  Fortinet appliances are automatically discovered by PCM. However, you must configure the following PCM setting for proper operation:

  NOTE: All discovered UTMs, regardless of vendor, are placed in the UTM folder in the PCM navigation tree. Although PCM discovers Fortinet appliances, they are not included in Network Maps. Instead, they appear in the unmanaged devices section.

  - If the UTM is configured with a unique read and write community name (other than PCM's default of "public"), configure the community names in PCM.
  - Configure the switch port connected to the UTM as a member of each VLAN where attacker or victim traffic might originate.

  For additional FortiGate UTM information, see the forthcoming Network Immunity Manager Implementation Guide (accessible by registering at my.procurve.com).

# PCM 2.2/2.2.1 Enhancements

## Update 4 Enhancements

- Wireless IDS support for  software version WS.02.07 of ProCurve Wireless Edge Services xl Module (WESM xl) and software version WT.01.02 of Wireless Edge Services zl Module (WESM zl). The WESM detects suspect behavior and sends traps to PCM (assuming PCM is registered as a trap receiver on the WESM). This allows the PCM user to identify the offender based on the Security Activity view and heat maps, however PCM cannot execute event-driven policies in response to the traps. Instead, actions based on these events are initiated by the WESM's mitigation features.

  For additional WESM wireless IDS information, see the ProCurve Wireless Edge Services Modules Management and Configuration Guide.

- Support for the ProCurve 8200zl switch, software version K.12.43.

- Support for the ProCurve Wireless Edge Services zl Module, which includes SNMPv3 communication. PCM can be used to configure WESMzl SNMPv3 communications settings in PCM but not on the device.

- Automatic update support for HP OV-NNM, which allows updating NNM configuration files for NNM support of new device traps and icons.

## Update 3 Enhancements

- IPS support for third-party UTM appliances from SonicWALL. These network security appliances prevent damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content.

- Support for ProCurve 2510-24G software version Q.11.xx and 2810-24G/2810-48G software version N.11.xx, which includes MAC auth and Web auth.

- Eleven Regulatory Compliance Reports were added:
  - Credential Change History
  - Device Access Configuration
  - Port Access Configuration
  - Device Access Password Audit
  - Device Access Credentials
  - Test Device Communication Results
  - Event Activity
  - Event Totals by Severity
  - Device Configuration Change History

- Device Configuration Change Totals
- Executed Policies

## Update 2 Enhancements

- Support for third-party FortiGate appliances from Fortinet. These network security appliances prevent damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, and inappropriate web content.
- Location of the Network Maps link labels have been moved closer to the device icons instead of centered over the links.
- A checkbox has been added to the Network Maps toolbar. If checked, node positions are preserved during discovery and client shutdown. If not checked, nodes are arranged in the default layout.
- Support has been added for the ProCurve 1800-24G-B switch.

## Update 1 Enhancements

No enhancements were included in Update 1.

# Software Fixes in PCM 2.2/2.2.1 Updates

Unless otherwise noted, each new release includes the software fixes added in all previous releases.

## Update 5

- **Security Activity (PR_1000431205)** — WESM xl radios (software version WS.02.08) are not listed in the Network ImmunityManager Security Activity tab. This PR requires PCM and Network Immunity Manager changes.

## Update 4

- **Dashboard (PR_1000423051)** — Incorrect model number for ProCurve 420 Access Point in PCM dashboard.
- **Discovery (PR_1000417720)** — PCM lists Cisco switches multiple times in the Devices List.
- **Port Speed (PR_1000440037)** — PCM lists wrong port speed for devices.
- **Traffic Monitor (PR_1000433958)** — PCM doesn't send out SNMP PDUs to a deleted device to unregister it, so the device continues to send sFlow samples and statistics.
- **Help (PR_1000447988)** — Help for Regulatory Compliance reports.
- **IDM (PR_1000451322)** — IDM stops displaying user login events.
- **License (PR_1000415182)** — Expiring license warning pop-under prevents access to main screen, which causes main PCM screen to appear frozen and not respond to mouse clicks.
- **ProCurve NAC 800 (PR_1000455632)** — PCM uses Telnet by default to communicate with the ProCurve NAC 800, which is not supported by the NAC. Also, PCM tries to communicate with the ProCurve NAC 800 using http. (The NAC only supports https.)
- **Web Agent (PR_1000458264)** — Web Agent uses Port 80 instead of port 443 for https.
- **Vulnerability (PR_1000457815)** — Remote exploitation of design error vulnerability in PCM could allow attackers the ability to access arbitrary files hosted on the PCM server.
- **Event Browser (PR_1000459657)** — Access violation traps use a period instead of a colon to separate hexadecimal digits.
- **MAC Lockout (PR_1000450735)** — Policy Manager allows the user to configure MAC lockout for a multicast address and does not warn the user that switches do not support this.
- **Software Update Wizard (PR_1000456972)** — When configuring the switch Software Update Wizard to perform an update in the future, the configured time is lost when the user clicks the Back button to return to the previous screen.

- **Power Units (PR_1000442094)** — Mobility Manager reports power output for the WESM xl in percentage instead of dBm.
- **Software Update Wizard (PR_1000450494)** — Cannot uncheck the Reboot button for 2510 switches.
- **Event Browser (PR_1000460367)** — WESM zl traps appear garbled in the Event Browser.

## Update 3

- **SSH (PR_1000438421)** — Add SSH support for NAC800.
- **Device Manager (PR_1000438222)** — System Contact and System Location fields in Device Manager System Info tab need to be longer to accommodate longer values supported by software version K.12.08.
- **Reports (PR_1000415579)** — No timestamps on Security reports.
- **MAC Address (PR_1000367396)** — MAC address is not properly displayed for traps sent by ProCurve 420, 520, and Wireless Edge Services xl Module.
- **Reports (PR_1000425192)** — Incorrect Auth State shown in Port Access Report.
- **Virus Throttling (PR_1000439695)** — Problem setting different port filter values at once for Virus Throttling.
- **Port Speed (PR_1000440037)** — Incorrect port speed for switches reported.
- **Software Update (PR_1000449148/1000435281)** — Scheduling of software updates fails when user returns to previous screens before clicking the Finish button, resulting in immediate updates.
- **Event Browser (PR_1000416920)** — New 3500/5400/6200/WESM traps are corrupted in PCM Event Browser.

## Update 2

The following PCM problems were resolved in PCM 2.2/2.2.1 Update 2

- **Mapping (PR_1000413209)** — Extra link lines in Network Map.
- **Event Manager (PR_1000416920)** — Some ProCurve Switch 3500, 5400, and 6200 traps are corrupted in the Event Browser.
- **Reports (PR_1000418406)** — “Error Generating Report” message box with no alerts included.
- **Mapping (PR_1000393281 and PR_1000411845)** — PCM doesn’t map devices after hardware replacement when the replacement has the same IP address.

- **Software Upgrade (PR_1000429809)** — Cannot perform a device firmware upgrade when switch is configured for SSH, SNMPv2, and TACACS.
- **MAC Lockout (PR_1000427416)** — When using MAC Lockout, dual entries are created for the same MAC address when locked via policies.
- **Mapping (PR_1000424352)** — Hierarchical layout button in Network Maps does not arrange device icons properly.
- **Policy Manager (PR_1000416815)** — On a client that is on a different PC than the server, Policy Manager does not always display the current enabled or disabled status of policies.
- **Syslog (PR_1000422419)** — Syslog performance issues.
- **Switch Config (PR_1000428592)** — In some cases, PCM triggers a switch NMI crash.
- **Discovery (PR_1000424310)** — Discovery performance improvements, specifically for large networks.
- **Software Update (PR_1000419926)** — User cannot select the version in the Software Update Wizard.
- **Traffic Manager (PR_1000419250)** — Offender Details lists an incorrect IP address for the offender. (Although Offender Details is part of Network Immunity Manager, PCM Traffic Manager is at fault.)
- **Templates (PR_1000415212 and PR_1000438213)** — When deploying a template to a 420 Access Point that has a new IP address, PCM can no longer manage the 420 Access Point.
- **Software Update (PR_1000435281)** — Scheduled firmware updates not working.
- **AD Synchronization (PR_1000433501)** — Active Directory Synchronization (ADSync) stops working when group or user account names contain special symbols.
- **Event Manager (PR_1000439684)** — Entries in the IDM Event Browser grow without limit.
- **Software Update (PR_1000439186)** — When using PCM to upgrade 2510 Switch software, user cannot select secondary flash.
- **Enhancement (PR_1000439687)** — SSL communication for Access Manager communications (including Secure Access Wizard, Port Access tab, and Virus Throttling configuration) between the client and server has been added.
- **Security (PR_1000429550)** — Internal Error: The alert object references missing capability = Security: ProCurve Alert.
- **Port Classification (PR_1000424392)** — In the Port Classification Dialog, the IP address are not in numeric order and there should be a Report Port column.
- **Firmware Update (PR_1000421026)** — Firmware update hangs if credentials are wrong in PCM.

# Update 1

The following PCM problems were resolved in PCM 2.2 Update 1

- **Auto-update (PR_1000426771)** — If PCM is installed with the Auto Update option set to "Download and Install Automatically", the Client may hang when it tries to download an Auto Update. To recover after a failed Auto Update attempt, restart the Management Service (in Windows Services) or reboot the Client PC and manually install the Auto Update.
- **AIO Failures (PR_1000437688)** — PCM reports "Login failed: No user manager server found" and various AIO failure codes.
- **Custom Groups (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.
- **Preferences (PR_1000439484)** — Blank page in Throttled event (Global:Event:Throttled:Events) from the Global Preferences window after an upgrade to PCM 2.2.