

Release Notes: ProCurve Management Software

ProCurve Manager Plus Version 3.0
Mobility Manager Version 3.0
Identity Driven Manager Version 3.0
Network Immunity Manager Version 2.0

PCM/PCM+ v3 New Features

For a description of the new features, FAQs, and what changed between PCM 2.x and 3.0 see:

<http://www.Procurve.com/pcmplus>

PCM (free version) Features, see

<http://www.Procurve.com/pcm>

For a list of license products, and which product to purchase, see

<http://www.Procurve.com/pcmplus-licensing>

For ProCurve Mobility Manager Features

<http://www.Procurve.com/pmm>

For NIM and IDM Information

<http://www.procurve.com/solutions/enterprise/security/security.htm>

To download free trial versions of PCM/PCM Plus and/or plug-ins, see:

http://www.hp.com/rnd/software/network_management.htm

ProCurve PCM Plus for HP Network Node Manager

ProCurve Manager integrates with HP Network Node Manager (version 7.5) to provide a robust solution for managing ProCurve network products in a multi-vendor environment. ProCurve Management is targeted for medium-sized enterprise networks to provide the PCM Plus functionality from the NNM interface, including ProCurve device management, network traffic monitoring, scheduled software updates, VLAN management, and policy management.

These release notes include information on the following:

- Installation Notes
- Known Issues

NOTE: These Release Notes are applicable at the date of the ProCurve Manager Version 3.0 Release. Please check the ProCurve Technical Support Web site at www.procurve.com for recent information.

© Copyright 2005 - 2007, 2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

5991-8605b
July, 2009

Applicable Products

ProCurve Manager v3.0
ProCurve Manager Plus v3.0
ProCurve Mobility Manager v3.0
ProCurve Identity Driven Manager v3.0
ProCurve Network Immunity Manager v2.0

Trademark Credits

Microsoft, Windows, Windows XP, and Windows Vista are registered trademarks of Microsoft Corporation.

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

The information contained in this document is subject to change without notice.

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.

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

Installation Notes

The installation download includes the base product PCM (free version). However at install time, the PCM+ trial version is installed, and after 60 days if not licensed, will revert to the PCM free version. The PCM Installer also provides the option to install plug-ins PMM 3.0, IDM 3.0, and NIM 2.0.

All plug-ins require PCM+ to operate. Since they are part of the trial, they too will stop operating after the 60-day trial. To continue using the plug-ins, you must purchase licenses for PCM+ and the plug-in. For more details about licensing, refer to the License and Upgrade paper located at:

<http://www.Procurve.com/pcmplus-licensing>

For Installation requirements and “how to” details, see the HP ProCurve Network Management, Installation and Getting Started Guide. (This includes the installation details for PCM 3, PCM+ 3, PMM 3, NIM 2, and IDM 3.

<http://www.Procurve.com/pcm-manuals>

Notes:

- All PCM/PCM Plus software and hardware installation requirements are listed in the Installation and Getting Started Guide. For other details on configuration, see HP ProCurve Manager 3.0 Network Administrator’s Guide, located on the same web page listed above.
 - ProCurve Management software is not localized for non-English versions of Windows.
-

Mobility Manager 2.0 Notes

- If the network contains access points that are not configured with the default CLI passwords and SNMP credentials used by PCM, 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.

Known Issues for PCM 3.0

The following are known problems that are new in PCM/PCM Plus 3.0. If you were using PCM 2.3, the known problems, called Problem Reports (PRs) from PCM 2.3, Auto Update 10 have been fixed in PCM/PCM Plus 3.0.

General

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

Agent Manager

- **(PR_18350)** — Moving Cisco devices across agents shows incorrect status for trap receiver configuration.
Workaround: Ignore the result since trap receiver configuration is not supported for Cisco devices
- **(PR_18069)** — The PCM remote agent is unable to establish a connection to the PCM server if the default agent group is deleted.
Workaround: do not delete the default agent group
- **(PR_17190)** — Deleting a remote agent from PCM does not delete the agent from Agent Map.
Workaround: Restart the PCM client solves the issue.
- **(PR_12656)** — The agent group icon in the left navigation tree displays inconsistent results between the default agent group and remote agent group when an agent is disconnected.

Agent Web User Interface

- **(PR_18714)** — Setting any of the four special characters, <, >, ‘, “ from the Agent Manager will cause the Agent Web UI to become unresponsive.
- **(PR_18710)** — From the Agent Web UI, setting \ character in the Agent name Description or Login fields causes the Agent Web UI to become unresponsive.
Workaround: Remove the \ character from the field that contains it.

Configuration Integration Utility

- **(PR_18439)** — Configurable Integration Platform (CIP) utility not functioning after adding Web application with a special “dot” character in the application name.
Workaround: Do not enter/use “.” in the application name.

- **(PR_18805)** — Configurable Integration Platform (CIP) utility does not support user defined profiles.

Workaround: CIP Utility supports the profiles of Administrator, Operator and Viewer.

Configuration Manager

- **(PR_17461)** — Software Configuration Scan in SCP mode fails to capture changes on HP ProCurve Secure Router 7203dl series if “write mem” was not performed on the device prior to scan.
- **(PR_17961)** — Configuration Manager is unable to perform a full scan of AP 420.
- **(PR_16241)** — PCM fails to perform any Configuration Manager and Software Update operations on the 7000 series when Manager & Operator Passwords are different.

Discovery

- When adding subnets for Discovery in Global Preferences, if an invalid IP address is used the subnet will not be discovered.
- **(PR_13279)** — PCM will not discover devices if a DNS name for the seed device is provided instead of the IP address.

Workaround: While discovering devices from any new subnet, use Manual Discovery Wizard or provide seed device IP address in “AgentManager->Discovery->seed IPaddress” field instead of a DNS name.

- **(PR_18352)** — Changing the device default communication parameters when rediscovering a device does not update the database with the new credentials.
Workaround: Use Device Manager->Communication parameters in PCM and set the correct SNMP/CLI credentials.
- **(PR_18133)** — After setting the Discovery-> Restrict to IP Address Range in the Agent Manger and restarting the agent causes discovery of devices outside of the required IP range.

Device Manager

- **(PR_16633)** — Test Communication Parameters may randomly fail.

Workaround: None at this time.

- **(PR_13676)** — When making changes in the Threat Management Services Module, In Device Manager -> Trap Receivers, "Modify Trap Receiver" and clicking OK, the Trap Receiver is deleted.

Workaround: Instead of using Modify Trap receiver option to modify the trap receiver, follow these steps:

1. First delete the trap receiver. Make sure it was deleted.

2. Add the trap receiver with new information.

Note: Only delete one trap receiver at a time. Multiple delete option and Delete all option are not be supported.

- **(PR_17281)** — In Port Classification screen, 'Remote Port' information does not display properly.

Workaround: None at this time.

- **(PR_18934)** — PCM CLI Wizard results in Switch 4100 becoming unresponsive to all management interfaces.

Workaround: None at this time. Switch reboot required to restore access.

- **(PR_15900)** — Adding user-defined devices to a user within a customized profile does not work properly. After re-launching the client, the devices are not displayed in the customized user profile.

Events Management

- **(PR_18694)** — Excessive bursts of "Security Access Violation" events from switch devices are being reported in PCM.

Workaround: Configure default SNMP read/write community in the switch. This may prevent excessive "Security Access Violations" events in PCM.

- **(PR_18426)** — Events->Default setting for syslog archival does not work properly.

Network Map

- **(PR_13293)** — Threat Management Services (TMS) Module is displayed as a disconnected object on the Network Map. Occurs when multiple TMS modules reside on the same switch.

- **(PR_18343)** — Agent Map does not display properly when switching between different layout views.

Workaround: Click on one of the layout toolbar buttons in the Agent Map explicitly.

- **(PR_11992)** — Network Map can appear 'flat' in networks that include complex connections, such as meshing.

Workaround: Try using the Uniform Length Edges layout format.

Installation

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

- **(PR_18674)** — PCM does not uninstall correctly after all plug-ins were uninstalled.

- **(PR_18610)** — PCM does not install properly when special characters are used in installation path.

Policy Manager

- **(PR_17745)** — Policy Manager "Send Email" action does not remove HTML tags in email notifications.
- **(PR_18349)** — Policy Manager History tab uses the filter selected for an individual device instead of all devices.
- **(PR_18222)** — Policy Manager may not send email alert notifications during peak server load times.
- **(PR_17831)** — Local PCM Client memory spikes and hangs after browsing on the Policy Manager Window when PCM server is supporting the maximum limit of agents and devices.

Reports

- **(PR_18814)** — When generating reports from the Main menu, the report footers are not displayed after restarting the client.
- **(PR_18438)** — Any report generated which includes the fields Port Status or Authentication Status, the data is displayed with incorrect format.

Traffic Manager

- **(PR_17733)** — Traffic Manager configures and displays port information for devices that do not support traffic collection.
- **(PR_17130)** — SNMP counters may display incorrect traffic information occasionally when using the ProCurve Switch 1700 series.

Known Issues for PMM 3.0

General

- **(PR_10753)** — In PMM 3.0 release, the parent WESM's IP address is incorrectly shown as Radio Port's IP addresses.
- **(PR_12599)** — Copy and paste does not work properly when drawing zones on floor maps in radio frequency visualization.
- **(PR_14208)** — Throughput history chart in main dashboard sometimes does not match devices throughput history table.
- **(PR_16087)** — Once a managed device without ROM, software version and/or, serial number is added to the radio frequency visualization floor map, it becomes difficult to set Location Confidence Configuration parameters for all other devices added to the floor map afterwards.

- **(PR_17115 and PR_37821)** — Sometimes when the devices are unreachable, their Associated Stations History chart can still show that there are stations associated to them.
- **(PR_17303)** — Sometimes PMM 3.0 cannot detect the mode for the radios. This can be resolved by rediscovering the troubled devices.

Known Issues for IDM 3.0

General

- **(PR_40822)** — The IDM 3.0 Agent can be installed on non-supported 64-bit platforms. If the IDM 3.0 Agent is accidentally installed on an unsupported 64-bit platform, such as Windows 2003-64bit, the RADIUS server will repeatedly crash. While IDM states support for only 32-bit Operating Systems, the IDM Agent installer does not prevent the installation on a 64-bit platform.

Workaround: The IDM 3.0 agent must be uninstalled from the 64-bit platform in order for the RADIUS server to recover. To uninstall the IDM Agent, go to the Start Menu, Select IDM Agent, and then Uninstall. After a successful uninstall, the RADIUS server will function normally.

- **(PR_42058)** — After installing a PCM Auto Update, the IDM event log may have entries that appear, starting with the following text: “Warn: Replaced non-printable characters with #...” This type of IDM event entries can be safely ignored and will be addressed in a future IDM Auto Update.

- **(PR_14162 and PR_15085)** — Redhat Enterprise Linux 5 agent installation may cause warnings from SELinux. During installation and auto update, SELinux may display warnings/errors to the user, even when they elect to install the policy provided during installation of the agent. The warnings can be ignored. The errors will break functionality.

Workaround: If the customer has not installed the SELinux policy provided with the agent installer, then they need to run `"/var/opt/HP/idm/bin/configSELinux.sh -e"` to enable the policy. They should then restart the radiusd service. If there are still problems, they likely have a newer version of the SELinux policy and will have to update the policy themselves, following the instructions provided by Redhat.

- **(PR_14929)** — User Import LDAP credential change requires PCM server restart In the User Import wizard, if external authentication credentials are used to successfully authenticate with an LDAP server, they cannot be changed without restarting the PCM server. This means that the next time the user runs the User Import wizard even if they enter a new keystore and password the original version is used.

Workaround: Restart the PCM service, then enter the new credentials.

- **(PR_14790 and PR_15117)** — User Import cannot import users from large groups. The User Import wizard may fail to import users if a group is selected to import which has a large number of users, usually greater than 1000.

Workaround: For Active Directory servers, the workaround is to use the User Directory Synchronization feature instead of User Import. Another possible workaround is to increase the MaxVal-Range to be large enough to accommodate the largest group you want to import from. See <http://support.microsoft.com/kb/315071> for more detailed instructions for changing this setting.

- **(PR_10598)** — PCM Server IP address change requires additional configuration on NAC. When upgrading to IDM 3.0 on the NAC, the user will be prompted for the PCM Server IP address. If the PCM Server IP address has changed from the previous value, the new value is not reflected in the Web UI of the NAC.

Workaround: To make sure the NAC is correctly configured, the user will have to change the PCM Server IP address via the NAC Web UI.

- **(PR_12068)** — RADIUS clients added with SAW can't be removed successfully via the NAC Web UI. After deleting a RADIUS client from the NAC800 Web UI which was added through the IDM Secure Access Wizard, users logging in from the deleted RADIUS client continue to be granted access because the RADIUS client is not removed from the NAC800 clients.conf file.

Workaround: Manually remove the RADIUS client from /etc/raddb/clients.conf on the NAC800

- **(PR_17899)** — LAD enable fails to take effect. If LAD is enabled and soon after a password is added to a pre-existing user, LAD may be disabled

Workaround: Disable and enable LAD again

- **(PR_12873)** — Client login fails authentication with WLAN access configured for AP420. If an access policy rule is configured with an AP420 as the WLAN, the clients connecting through the AP420 will fail authentication. This behavior is due to a defect in the AP420 software, and the AP420 team has been notified.

Workaround: There is no work around for this in IDM as there is no other way to retrieve the SSID from the RADIUS packet. A software update is not currently available for the AP420 to fix the problem.

- **(PR_14274)** — Access policy for user is not applied correctly to switch with Suse 9.3, 10 and RedHat 4 IDM agents. The user seems to be authenticated successfully, but the switch does not apply the correct access policy attributes that were configured in IDM. There is a defect in FreeRADIUS 1.0.0 - 1.1.0 for the "use_tunneled_reply" flag in the PEAP configuration section of eap.conf. Certain supplicants such as Juniper Odyssey and Xsupplicant require this flag, along with "copy_request_to_tunnel" in order to operate correctly and thus are more likely to see this issue.

Workaround: If supplicant does not require "use_tunneled_reply", remove from eap.conf. Otherwise, upgrade to FreeRADIUS 1.1.1 or later.

- **(PR_17135)** — Cisco VoIP Phones using 802.1x to authenticate with Microsoft IAS do not have IDM policy applied or do not show correct login status. Cisco VoIP phones have hard-coded usernames that are longer than Active Directory allows, so IAS cannot authenticate them.

Workaround: Modify IAS request processing to remove the first 9 characters (model number) from the user name for the Cisco VoIP phones. Side effect of this change is that IDM will no longer be able to show correct login status because the username does not match the RADIUS accounting packet. Another workaround is to use MAC-auth instead.

- **(PR_17310)** — Mitel and/or Cisco VoIP Phones do not authenticate successfully after power cycle. When a PC is attached to the PC Port of a Mitel or Cisco VoIP phone, after the switch or phone is power cycled, the phone authenticates forever until the power is removed and the PC is unplugged from the PC port. The RADIUS Assigned Tagged VLAN fails to get assigned when there is a PC authenticated and attached to the PC Port of the phone. The PC always authenticates first and causes a failure in the phone to boot as the switch never applies the tagged VLAN from IDM. An event log message appears:

```
W 02/05/09 13:39:00 02403 dca: 8021X client tagged VLANs arbitration error, MAC
08000F383213 port 12.
```

This scenario can potentially occur when the phone or switch is power-cycled due to firmware upgrades or loss of power.

Workaround: Remove the PC attached to the phone PC port so that the phone can receive its tagged VLAN assignment first. After the phone is fully operational and can receive a dial tone from the PBX, attach the PC to the phone and the PC may authenticate separately.

- **(PR_14275)** — NIM mitigated users do not have existing IDM policy applied. When using NIM with IDM integration, if a user is mitigated by NIM any existing IDM policy attributes for the user are not applied. For example, if the NIM mitigation rule applies a rate limit but IDM was configured to place the user in a specific VLAN, when the user next authenticates the NIM rate limit is applied but not the vlan.

Workaround: Configure NIM policy to include vlan attribute in addition to rate limit.

- **(PR_15999)** — IDM agent and radiusd do not start on Suse 10.2 VMWare Virtual Machine. After installing IDM on Suse 10.2 VMWare virtual machine that was created using the export/import utility, the idmagent and radiusd services are not started, and a Java JRE warning appears.

Workaround: Manually configure the correct Guest Operating System setting

1. Shutdown the SuSE 10.2 VMware image that exhibits the installation failure.
2. Wait for it to totally power down.
3. Right click on the SuSE 10.2 VMware image that exhibits the installation failure.
4. Click on “Edit settings...” in the drop-down list.
5. Click on the “Options” tab.
6. Click on “General Options” under the “Settings” heading.
7. Select “(o) Linux” under the “Guest Operating System” configuration pane.

8. Select “Suse Linux Enterprise Server 10 (32-bit)” in the “Version:” drop-down list.
9. Click on “[OK]”.
10. Power on the VM.

- **(PR_17565)** — Secure Access Wizard displays "Communication with the RADIUS server failed". When using the Secure Access Wizard to configure RADIUS clients, if an unsupported RADIUS server is entered (i.e., a FreeRADIUS server) the error is shown.

Workaround: RADIUS clients must be added to FreeRADIUS servers manually

- **(PR_18199)** — Secure Access Wizard or Adding RADIUS Clients Wizard displays failed status when AP530 Devices are selected. When using the Secure Access Wizard or Adding RADIUS Clients Wizard to configure AP530 devices, the status column displays a failed status. The operation log displays "Communication with the device failed" However, the device configuration actually succeeds so the error message may be disregarded.

Workaround: Increase the SNMP timeout to 30 seconds for AP530 Devices

- **(PR_18178)** — Changing Single User target in Global Rule does not automatically deploy to agent(s). If automatic deploy is enabled and an existing Global Rule Single User target is changed to a new user, the policy is not automatically deployed to the IDM agent(s)

Workaround: Deploy policy to realm manually

Known Issues for NIM 2.0

General

- **(PR_18110)** — The NBAD Status and Top Offenders chicklets (perhaps others) are not refreshing until the NIM Dashboard is unselected and subsequently reselected.

Workaround: Select another tab, then select NIM dashboard tab again

- **(PR_17345)** — The Security Activity tab does not refresh unless actively in use.

Workaround: Select a different subtab (Offenders, Alerts, Actions) then reselect the tab

- **(PR_17167)** — DHCP Snooping events are incorrectly setting fields to "Unresolvable DNS Name" which causes Alerts to incorrectly display this as offender.

- **(PR_17636)** — Can't see all bars on Security Activity tab's horizontal stacked bar chart.

Workaround: Hovering the mouse over a bar will display the stacked bar segment counts in a tooltip

- **(PR_18167)** — NIM Dashboard Device Troublespots Agent Identities are wrong.

- **(PR_17833)** — For switches that do not support Data Center Automation, rollback of the Quarantine VLAN Action fails.

Release Notes: ProCurve Management Software
Known Issues for NIM 2.0

- **(PR_17681)** — For Data Center Automation-supported switches, rollback of the Quarantine VLAN action should delete the newly created VLAN and the previous port assignment of VLAN should be restored.
- **(PR_17292)** — When the “Connect” or “SYN” scans are performed no NBAD events are reported.
- **(PR_17752)** — Change wording of Events tab right-click menu choice "Exclude security monitoring" and other strings.
- **(PR_18216)** — The Alerts by Device and Offender report does not consolidate rows showing the same data, but with different counts.
- **(PR_18327)** — The Network Activity by Offender IP Range report is not limiting Offenders to specified IP range, and uses the obsoleted, NIM 1.x, “External” types of alerts.
- **(PR_18198)** — Actions by Policy Name report labels alerts with wrong type, maps values to columns incorrectly.
- **(PR_18224)** — Most Active Alerts report uses obsoleted alert types.
- **(PR_18214)** — Alert Distribution by Device report uses obsolete alert types.
- **(PR_18219)** — Security Alerts Not Handled by Policies report shows obsolete alert types.
- **(PR_13320)** — Security totals shown on maps don't seem to be right.
- **(PR_18923)** — TMS manager- IPS Traps not decoded properly.
- **(PR_18326)** — The “Null” value is displaying as a DNS name in the Network Map of the NBAD Wizard.
- **(PR_18903)** — NIM Monitoring tab’s Help does not work.
- **(PR_18664)** — The NIM Add Exclusion Entry/Entries dialogs and Find Exclusion should use the terms "Offender" instead of "Src" (Source) and "Victim" instead of Dst (Destination).
- **(PR_17562)** — Wrong Validations in the “Suggested Actions” step of NBAD Wizard
- **(PR_1816320)** — Automatically exclude PCM agent from alerts when a switch is sending SNMP authorization traps using K.13 switch software.