

Release Notes: ProCurve Network Immunity Manager Version 2.0, Update 2

ProCurve Network Immunity Manager (NIM) version 2.0, Update 2 supports these products:

- J9161 HP ProCurve Network Immunity Manager 2.0 - 50-device license
- J9162A HP ProCurve Network Immunity Manager 2.0 - +100-device license
- J9163A ProCurve Network Immunity Manager 2.0 - unlimited device license

Network Immunity Manager is an add-on module to PCM+ 3.0 or later. If you are using a version of PCM or PCM+ earlier than PCM 3.0, you must first upgrade to PCM 3.0 before you can apply the fixes included in this update.

These release notes include information on the following:

- Software Management ([Page 3](#))
- NIM Notes ([Page 5](#))
- Enhancements included in the Auto-Update releases. ([Page 6](#))
- Software fixes included in the Auto-Update releases. ([Page 7](#))
- Known issues included in the Auto-Update releases. ([Page 13](#))

Related Publications

For the latest version of any of the publications listed below, visit the ProCurve Networking Web site at www.hp.com/go/procurve/manuals.

- *HP ProCurve Network Immunity Manager Security Administrator's Guide, Version 2.0*
- *Read Me First for the ProCurve Manager, Version 3.0*
- *HP ProCurve Network Management Installation and Getting Started Guide*
- *HP ProCurve Manager Plus 3.0 Network Administrator's Guide*
- *HP ProCurve Network Management 3.0 Migration Guide*

© Copyright 2005 - 2009

Hewlett-Packard Development Company, LP.

The information contained herein is subject to change without notice.

Publication Number

5991-8587

September, 2009

Applicable Products

- J9161A ProCurve Network Immunity Manager 2.0 - 50-device license
- J9162A ProCurve Network Immunity Manager 2.0 - +100-device license
- J9163A ProCurve Network Immunity Manager 2.0 - unlimited 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](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.hp.com/go/procurve


Software Management – NIM 2.0 Update 2

ProCurve Manager 3.0 Update 4 must be installed before installing this ProCurve Network Immunity Manager 2.0 update. Once you have installed the ProCurve Manager update, you can install this update using the “Automatic Update” feature in PCM+, or you can install it manually.

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


[Tools->Preferences...->Global->Automatic Updates->Update History]

Using Automatic Download and Install

1. Click the  Preferences button on the global toolbar to open the Preferences window and select **Auto Updates for PCM** in the left pane of the Preferences window.
2. In the right pane, select Download and install automatically.
3. To change the schedule when PCM checks for automatic updates, set the Recurrence pattern.
4. Click **Apply** to save your changes and leave the Preferences window open or click **OK** to save your changes and close the Preferences window.


PCM checks the ProCurve FTP server for updates at the scheduled time. If updates are found for PCM or an installed module, PCM automatically downloads and installs the updates.

Using Notify if Updates Are Available

1. Click the  Preferences button on the global toolbar to open the Preferences window and select **Auto Updates for PCM** in the left pane of the Preferences window.
2. In the right pane, select Notify if updates are available.
3. To change the schedule when PCM checks for automatic updates, set the Recurrence pattern.
4. Click **Apply** to save your changes and leave the Preferences window open or click **OK** to save your changes and close the Preferences window.

PCM checks the ProCurve FTP server for updates at the scheduled time. If updates are found for PCM or an installed module, PCM issues an Automatic Update event (shown on the Agent Groups Events tab). Updates are not installed automatically. To install updates, you must manually initiate the download, as explained below.

Manually Installing Updates from the FTP Server

1. Click the  Preferences button on the global toolbar to open the Preferences window and select **Auto Updates for PCM** in the left pane of the Preferences window.
2. In the right pane, click **Check Now**.

3. In the Select Update Mode window, select the Check for updates on the FTP Server option and click **Next**.

PCM must be connected to the internet and, if using a proxy, it must be configured in Network Settings preferences.

4. Available updates are displayed with a check next to each one, which indicates that the update will be installed. Click **Next** to install the update, or if you do not want to install an update, uncheck the box.
5. A warning message appears, advising you that any PCM clients will be disconnected. Click **Yes** to continue.
6. After the update package is downloaded, you will be prompted to close the PCM Client. Click **Exit** to exit PCM, complete the update, and restart the PCM services.


You can then restart the PCM client and begin using the updated version of PCM.

Manually Installing Updates from the Download Folder

This method does not require an internet connection from PCM. The update can be downloaded from any PC and copied to the PC containing PCM.

1. Determine the PCM software version by selecting Help>About ProCurve Manager from the PCM menu.
2. Copy the nim_2_0_update_2.zip file to the \PNM\server\data\download\autoupdate directory. The default PCM server installation directory is: C:\Program Files\Hewlett-Packard\PNM\server on the workstation where PCM was initially installed. (Do not unzip the file.)

Update files can be downloaded from www.procurve.com/networkmanagement using any PC and copied to the PC containing PCM.

3. Click the  Preferences button on the global toolbar to open the Preferences window and select **Auto Updates for PCM** in the left pane of the Preferences window.
4. In the right pane, click **Check Now**.
5. In the Select Update Mode window, select the Check for updates in PCM's download folder option and click **Next**.
6. Available updates in the autoupdate folder are displayed with a check next to each one, which indicates that the update will be installed. Click **Next** to install the update, or if you do not want to install an update, uncheck the box.
7. A warning message appears, advising you that any PCM clients will be disconnected. Click **Yes** to continue.
8. After the updates are installed, you will be prompted to close the PCM Client. If you do not exit PCM manually, after a few moments PCM automatically shuts down. Click **Exit** to exit PCM, complete the update, and restart the PCM services.

You can then restart the PCM client and begin using the updated version of PCM.

NIM Notes

Update 1

SNMP Authentication Traps

As of NIM AU1, SNMP authentication traps are added to the default NIM exclusion list for Agents created after NIM AU1 is installed. However, the exclusion list for existing Agents is not altered, so you must manually add SNMP traps to the Agent's exclusion list if you want the Agent to exclude them.

NIM 2.0 Enhancements

Update 2

NIM 2.0 Auto Update 2 does not include any enhancements.

Update 1

- McAfee IPS support.
- Fortinet OS 4.0 support.
- Events tab right-click menu choice “Exclude security monitoring” renamed to “Exclude offender from security analysis”.
- The following report names have been changed:
 - Most Enforced Security Actions report renamed to Action Distribution by Device (Also MAC Mirror Actions column added and alert records that didn’t evoke a mitigation action eliminated).
 - Alerts Not Handled by Policies report renamed to Alerts that did not Invoke Actions.
- On NIM Configuration panel, “Less events” was changed to “Fewer Events”.
- On NIM exclusions screens, the source is now shown as offender.
- Traffic Analyzed column heading in the NBAD Analyzer Status pane of the NIM Dashboard was changed to "Relevant Traffic Observed".
- NBAD statistics changed to show maximum false positives per hour instead of probabilities.
- Improved detection of mass emailing worms.
- UDP DNS MX Query anomaly is generated when any MX requests are found in DNS frames of 128 bytes or less.
- Enhanced TCP Port Sweep algorithm that caused certain port scans to remain undetected (cleaned up and reduced usage of getTcpScanTypeCounts function call, because it did not properly match certain packets which needed to be detected)
- Enhanced NBAD to check for an obscure case where the primary TCP scan type is other than SYN scan. This enhancement results in simpler but less accurate magnitude checks.

Software Fixes in NIM Updates

Update 2

- **NBAD (PR_42894)** — NBAD does not detect the Bagle email virus.
- **NIM Preferences (PR_43710)** — NIM Exclusion lists NBAD entries as IPv6 address.
- **NBAD (PR_41652)** — No NBAD Rogue NAT event when port marked as Edge.

Update 1

- **Dashboard (PR_18110)** — The NBAD Status and Top Offenders Chicklets (and perhaps others) are not refreshing until the NIM Dashboard is unselected and subsequently reselected.
- **Security Activity Tab (PR_17345)** — The Security Activity tab does not refresh unless actively in use.
- **Offenders Tab (PR_41050)** — SAT Offenders tab either fails to load offenders or client hangs if it loads.
- **Security Activity Tab (PR_17636)** — Can't see all bars on Security Activity tab's horizontal stacked bar chart.
- **NBAD Wizard (PR_41515)** — NBAD Event Diagnostics wizard does not display the description part for UDP DNS MX Record query Protocol anomaly event.
- **NBAD Wizard (PR_40896)** — Only the "Exclude event" and "No action" options are available for the NBAD Wizard.
- **Network Map (PR_39736)** — PCM Client [Network Map] hangs for at least 10 minutes when Time Span is 500 hours for Device View=Security state.
- **NBAD Wizard (PR_18326)** — The Null value is displayed as a DNS in the Network Map of the NBAD Wizard.
- **Help (PR_18903)** — No help provided for NIM Monitoring tab.
- **NBAD Wizard (PR_17562)** — Usability issues with the Suggested Actions step of the NBAD Event Diagnostics Wizard.
- **Alerts by Device and Offender Report (PR_18216)** — Alerts by Device and Offender report has rows that show the same data but with different counts.
- **Network Activity by Offender IP Range Report (PR_18327)** — Network Activity by Offender IP Range report is not limiting offenders to specified IP range and uses obsolete alert types.

- **Event Activity Report (PR_18201)** — Event Activity report data does not contain security event content.
- **Actions by Policy Name Report (PR_18198)** — Actions by Policy Name report labels alerts with wrong type and maps values to columns incorrectly.
- **Most Active Alerts Report (PR_18224)** — Most Active Alerts report uses obsolete alert types.
- **Alert Distribution by Device Report (PR_18214)** — Alert Distribution by Device report uses obsolete alert types.
- **Security Alerts Not Handled by Policies Report (PR_18219)** — Security Alerts Not Handled by Policies report shows obsolete alert types.
- **Security Alert Activities Report (PR_40010)** — Security Alert Activities report displays Alert Type as External and Mitigation Action Status as New (in NIM 2.0 External is replaced by Non-ProCurve terminology).
- **Most Active Offenders and Alerts by Severity Report (PR_40486)** — Most Active Offenders and Alerts by Severity report is inaccurate.
- **Network Maps (PR_13320)** — Security totals shown on maps are not correct.
- **NIM Preferences (PR_17656)** — Text describing Preference setting's effect for NIM-IDM integration is not descriptive.
- **Authorization Traps (PR_16320)** — Automatically exclude PCM Agent from alerts resulting from Titan 3 SNMP authorization traps.

Workaround: Resolution requires users to perform the following steps before the IP address sweep exclusion is reapplied with the SNMP Auth exclusion:
 1. Remove PCM Agent's exclusion for IP address sweep.
 2. Restart the PCM Server (not PCM Agent).
- **ICMP Anomalies (PR_17237 & 17242)** — The isRelevant should also include packets of IP protocol for certain ICMP anomalies since some ICMP anomalies are flagged as IP traffic.
- **NBAD Events (PR_17292)** — NBAD events are not generated for Connect and SYN scans. An NBAD event can only be generated if the offender is sending more SYN flags than the victim and sending fewer responses (defined as ACK + ACK/RST flags) than the victim. Some FINEST level debug logging has been added to map the TCP flow state data so the problem can be patched easier if it happens again under different circumstances.
- **NBAD Events (PR_17167)** — DHCP Snooping events are incorrectly setting fields to "Unresolvable DNS Name" which causes Alerts to incorrectly display this as offender.
- **Security Activity Tab (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.
- **Quarantine VLAN (PR_17833)** — For switches that do not support Dynamic Configuration Arbiter, rollback of the Quarantine VLAN Action fails.
- **Quarantine VLAN (PR_17681)** — For Dynamic Configuration Arbiter-supported switches, rollback of the Quarantine VLAN action should delete the newly created VLAN and the previous port assignment of VLAN should be restored.
- **NBAD Events (PR_17292)** — When the “Connect” or “SYN” scans are performed no NBAD events are reported.
- **Events Tab (PR_17752)** — Change wording of Events tab right-click menu choice "Exclude security monitoring" and other strings.
- **Alerts by Device and Offender Report (PR_18216)** — The Alerts by Device and Offender report does not consolidate rows showing the same data, but with different counts.
- **Network Activity by Offender IP Range Report (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.
- **Actions by Policy Name Report (PR_18198)** — Actions by Policy Name report labels alerts with wrong type, maps values to columns incorrectly.
- **Most Active Alerts Report (PR_18224)** — Most Active Alerts report uses obsoleted alert types.
- **Alert Distribution by Device Report (PR_18214)** — Alert Distribution by Device report uses obsolete alert types.
- **Security Alerts Not Handled by Policies Report (PR_18219)** — Security Alerts Not Handled by Policies report shows obsolete alert types.
- **Network Maps (PR_13320)** — Security totals shown on maps don't seem to be right.
- **NBAD Wizard (PR_18326)** — The “Null” value is displaying as a DNS name in the Network Map of the NBAD Wizard.
- **Help (PR_18903)** — NIM Monitoring tab’s Help does not work.
- **Add/Find Exclusion (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).
- **NBAD Wizard (PR_17562)** — Wrong Validations in the “Suggested Actions” step of NBAD Wizard
- **NullPointerException (PR_17562)** — NullPointerException occurs when NIM server is restarted.

- **HA Clusters (PR_18050)** — RC Build 102: If the TMS zl module is in Monitor Mode, the TMS-HA>Add Device to Cluster option is enabled in the right-click menu and the device is listed in the Available Devices list on the Select Devices to be Clustered page of the Create Cluster Wizard.
- **Quarantine VLAN (PR_17680)** — RC Build 101: When quarantining a VLAN action for DCA supported switches, rollback is successful (DCA bind is reverted), but the rollback result is shown as “Failed to rollback VLAN settings”.
- **TMS HA Clusters (PR_14059)** — Under TMS-HA Clusters tab, the “Show this tab in a new window” does not work.
- **Navigation tree (PR_14844)** — Device tree TMS-Module right-click menu items grouped together.
- **Help (PR_14959)** — No help page available for the TMS Named Object Wizard “Modify or Delete Address, service groups”.
- **TMS Zone Wizard (PR_15047)** — Expand VLANs in Zone Wizard VLAN configuration sequence by default when few VLANs are selected.
- **TMS User Wizard (PR_15189)** — Most information is not updated or refreshed automatically after configuration changes done through the User Wizard
- **TMS Named Object Wizard (PR_15923)** — Incorrect validation and option provided in Named Object Wizard. Should not be able to change from multi to single.
- **TMS Named Object Wizard (PR_15924)** — In Named Object Wizard, user cannot create/modify multi-entry named object with one entry.
- **TMS Named Object Wizard (PR_16024)** — Named Object modify operation for address object fails for multi-entry named object.
- **TMS Multicast Access Policies (PR_16724)** — PCM client crashes due to long notes entered in multicast access policies notes field.
- **TMS Cluster Wizards (PR_16845)** — Cancel button in the Applying Settings page of Add Device to Cluster, Create Cluster, and Modify Cluster Wizards does not work as expected.
- **TMS Reports (PR_16846)** — Sometimes the graph report output is not displayed (blank) for Top 10 Allowed Services and Top 10 Allowed Users by Connection to Zone Reports or is incomplete for List of Filters for Top 10 Allowed Users by Connection from Zone Report.
- **User Wizard (PR_17181)** — Sometimes ArrayIndexOutOfBounds exception is seen on client console while moving GroupsNodes between AvailableGroups and SelectedGroups in User Wizard>Remove User Group>Group Object Select Panel.
- **Synchronization (PR_17182)** — TMS Manager secondary discovery and synchronization is not working.
- **Firewall Tabs (PR_17258)** — Not all devices are listed across some Firewall tabs.
- **Port Map (PR_17265)** — TMS Manager Port Map services with UDP protocol are failing.

- **Create Cluster Wizard (PR_17449)** — In Applying Settings page of Create Cluster Wizard, clicking the Summary button does not display the Status Summary dialog.
- **Signatures (PR_17599)** — Synchronizing signatures not updating server and client in some conditions.
- **Firewall Rules (PR_17675)** — Incorrect message displayed regarding the estimated time to delete a large number of firewall rules.
- **Users (PR_17813)** — Cannot add firewall users easily in TMS Manager.
- **Users (PR_17821)** — Firewall users and schedules are not updated in TMS Manager GUI.
- **Firewall Schedules Wizard (PR_17822)** — No data validation in Firewall Schedules Wizard.
- **User Wizard (PR_17921)** — No client side validation for User Name field in User Wizard.
- **Reports (PR_18055)** — Top 10 Allowed Services report not sorted in descending order correctly.
- **TMS NAT Wizards (PR_18356)** — Remove self zone in NAT Wizards.
- **TMS Service/Address Group (PR_18357)** — Service/Address Group addition is successful even without specifying the group name.
- **TMS Service/Address (PR_18360)** — Service/Address can be deleted even when they are part of a firewall policy.
- **TMS Reports (PR_18422)** — Top Denied Services report not sorted properly in descending order.
- **TMS Reports (PR_18424)** — Sometimes Top 10 Denied Services report displays empty graph report.
- **TMS Reports (PR_18428)** — In Firewall Activity reports tabular column report lay, Policy ID with value 0 is displayed.
- **TMS Cluster Wizards (PR_18433)** — Create a New High-Availability Cluster page of Add Device to Cluster Wizard and Update the Properties of High-Availability Cluster page of Modify Cluster Wizard are not retaining the data entered when Back button is clicked.
- **TMS Modify Cluster Wizard (PR_18609)** — Sometimes Modify Cluster Wizard fails during Applying Settings the “Status: Failed” and “Reason:error:agent to device communication error” messages are shown.
- **TMS Modify Cluster Wizard (PR_18614)** — Sometimes the Modify Cluster Wizard is not rebooting the Participant device in a cluster.
- **TMS Configuration Wizard (PR_18677)** — Unexpected error message is thrown when adding custom connection time out in the Configuration Wizard.
- **TMS IPS traps (PR_18923)** — IPS traps not decoded properly.

Release Notes: ProCurve Network Immunity Manager Version 2.0, Update 2
Software Fixes in NIM Updates

- **TMS Signatures (PR_37434)** — Changes to IPS actions should change the action field in the IPS signatures.
- **TMS Network Disconnect (PR_38020)** — Network disconnect operations (e.g., device reboot and no high-availability) not working.
- **TMS (PR_38027)** — Firewall wizards do not support configurations with names containing # character (TMS zl module patch ST.1.0.090311).
- **TMS User Authentication (PR_38028)** — Local user authentication traps are not decode properly.

Known Issues for NIM 2.0

Update 2

No known issues for NIM 2.0 Auto Update 2.

Update 1

- **Traffic (PR_41652)** — The Rogue NAT event is not being detected when the port is marked as Edge by PCM. To fix this problem some changes must be made to the Traffic Collector in PCM.
- **NBAD (PR_42894)** — NBAD does not detect the Bagle email virus.
- **Auto Update (PR_42737)** — Auto Update fails to display error message, logs an exception for descrip.prp dependency field.
- **Log Settings (PR_15721)** — Ability to configure log settings of TMS zl module in TMS Manager.
- **Dashboard (PR_18231)** — The TMS Events Graph in the ProCurve TMS zl Device Group Dashboard always shows HA Events as 0.
- **Named Objects Wizard (PR_39534)** — TMS AU1 Build 42 - Named Object configuration wizards accepts special characters which are not supported in Device.
- **Firewall Properties Wizard (PR_39542)** — TMS AU1 Build 42 - Firewall Properties values and settings in Firewall Properties wizard are not in sync with the device properties values.
- **Firewall Properties Wizard (PR_39548)** — NIM 2.0 TMS AU1 - Build 42 - Firewall Properties Wizard - Custom Connection time out property configuration does not report error message for adding duplicate names.
- **Wizards (PR_39552)** — NIM2.0 - Commit changes option in all the TMS-mgr wizards should do HA-synchronization if the device is in a HA-cluster.
- **Firewall Properties Wizard (PR_39553)** — NIM 2.0 AU1- Firewall Properties Wizard-Port Maps, No check is there if a user wants to add a duplicate Port Map.
- **HA Clusters (PR_39684)** — NIM AU1- Cluster information is not shown properly unless TMS-synchronization is done.
- **Signatures (PR_39926)** — NIM 2.0 AU1 Build 67: Sometimes the TMS-IPS Tab -> "Signatures" Subtab of a ProCurve TMSzl module shows no signatures even when the device is having signatures. The TMS-IPSServer.log shows "Could not receive signature family/list".
- **HA Clusters (PR_39928)** — NIM AU1-Build 67-HA- When the master device goes down-cluster member information is showing same data for both the devices in the cluster.

Release Notes: ProCurve Network Immunity Manager Version 2.0, Update 2
Known Issues for NIM 2.0

- **ACL (PR_41263)** — NIM 2.0 AU1: Unexpected Shim Header and Mpkt errors with ACL.
- **Synchronize TMS Properties (PR_40775)** — NIM 2.0 AU1: Synchronize TMS Properties>IPS failing - Status showing Reason: Could not update properties for ShowIps.
- **TMS-HA Tab (PR_42027)** — NIM 2.0 TMS-HA tab shows no cluster when participant device is deleted from TMS Manager and HA is removed from Master device.
- **HA Cluster Wizards (PR_11688)** — Create a new Cluster action in the Create a Cluster Wizard and Add Device to Cluster Wizard accepts the same VLAN ID as the TMS VLAN (IP address).