



Release Notes: ProCurve Identity Driven Manager

Version 2.3

ProCurve Identity Driven Manager 2.3 (IDM 2.3) is a free upgrade from IDM 2.x. Before upgrading to IDM 2., you must upgrade to IDM 2.15.

For IDM 2.3, 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 2.1 base product - 500-user license
- J9013A ProCurve Identity Driven Manager 2.1 base product - upgrade from IDM 1.x to IDM 2.2, 500-user license
- J9014A ProCurve Identity Driven Manager 2.1 additional 2000-user license

Free Trial Versions

This compressed, ZIP-format file contains a 30-day free trial.

These release notes include information on the following:

- New Features
- IDM Notes
- Other Known Issues

NOTE: These Release Notes are applicable at the date of the ProCurve IDM Version 2.3 Release. Please check the ProCurve Technical Support Web site at www.procurve.com for more recent information.

© Copyright 2005 - 2008 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

5991-4729
May, 2008

Applicable Products

ProCurve Manager v2.3
ProCurve Manager Plus v2.3
ProCurve Mobility Manager v2.0
ProCurve Identity Driven Manager v2.3
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

New Features

Below is a summary of the new features that are available in ProCurve IDM with this release. Please refer to the ProCurve Identity Driven Manager 2.3 Administrator's Guide for a full description on the use of these features:

■ **IDM - NPS/NAP Integration**

IDM integrates with Network Policy Server (NPS), Microsoft's RADIUS server on a Windows 2008 server, and Network Access Protection (NAP), an Endpoint Integrity offering from Microsoft that is offered as an integrated solution in the following tiers:

- Server tier that runs only on NPS in Windows 2008
- Client tier that performs endpoint testing in Windows Vista

■ **Support for nested groups in Active Directory Synchronization**

Active Directory synchronization now includes all users who are indirect members of a group via intervening nested group relationships. For additional information, see 2-40.

■ **Enhanced Secure Access Wizard**

- AP530 Group Configuration Check Step has been added to support AP530 access points.
- Ports to which the secure access settings will apply can now be selected from a list.
- VLANs used for authenticated and unauthenticated ports can now be selected for 802.1X, Web Auth, and MAC Auth settings.
- Redirect URL has been added to redirect users who have logged in successfully.

IDM 2.3 Notes

- If you are installing IDM 2.3 or upgrading from previous versions to IDM 2.3, you must also install/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>. If installing the IDM Agent for Windows (IAS or Funk's Steel Belted RADIUS), simply double-click on the downloaded install.exe file. If installing the IDM Agent for freeRADIUS, extract the downloaded zipped files and double-click the install.sh file in the Red Hat or SuSE console_installation folder.
- 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 the "Reset accounting statistics" link.

Release Notes: ProCurve Identity Driven Manager

IDM 2.3 Notes

- 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 a 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
 - Rate limiting for all IDM freeRADIUS agents is incorrectly configured. This misconfiguration sets port bandwidth on a freeRADIUS authenticated port to 100% regardless of what bandwidth is specified in IDM. If bandwidth is set to no-override in IDM, bandwidth is left

at whatever the port is configured for. This is due to the incorrect datatype (string instead of integer) being set in the HP freeRADIUS dictionary (dictionary.hp). To fix this, change the datatype to integer as follows:

Please note that the radiusd process must be briefly stopped and started during this process.

1. Locate the existing dictionary.hp file using the find or locate commands from the shell of the linux system (e.g., `locate dictionary.hp` or `find / -name dictionary.hp`).

2. Stop radiusd:

```
service radiusd stop or /etc/init.d/radiusd stop
```

3. Backup the existing dictionary.hp:

```
cp /usr/share/freeradius/dictionary.hp /usr/share/freeradius/dictionary.bak
```

4. Edit the file located in step (1), e.g.

```
vi /usr/share/freeradius/dictionary.hp
```

5. Change the lines that look like:

```
ATTRIBUTE HP-bandwidth-max-ingress 46 string HP  
ATTRIBUTE HP-bandwidth-max-egress 48 string HP
```

To:

```
ATTRIBUTE HP-bandwidth-max-ingress 46 integer HP  
ATTRIBUTE HP-bandwidth-max-egress 48 integer HP
```

6. Start radiusd (e.g., `service radiusd start` or `/etc/init.d/radiusd start`)

Known Issues for IDM 2.3

- **Event Monitoring (PR_1000451322)** — When the same user logs in with 8 different MAC addresses, it exceeds the column size attribute of 100 and causes the event monitoring thread to abort with an exception. To resolve this issue, install IDM 2.2 Automatic Update 1 prior to installing IDM 2.3.
- **Discovery (PR_1000773616)** — Discovery initially discovers and places NAC 800 in RADIUS folders. After 30 seconds, the NAC 800 will be categorized correctly.
- **Windows Server 2008 (PR_1000765394)** — On Windows Server 2008 with 82566DM Gigabit Network Connection Card, communication cannot be established between the IDM server and the IDM agent, irrespective of firewall state.

Software Fixes in IDM 2.3

The following problems are resolved in IDM 2.3:

- **NetMgmt (PR_1000457752)** — Rate limiting is broken in IDM freeRADIUS agents.