



Release Notes: ProCurve Identity Driven Manager Version 3.0, Update 1

ProCurve Identity Driven Manager (IDM) version 3.0, Update 1 (C.03.00.339) supports these products:

- J9438A ProCurve Identity Driven Manager 3.0 base product - 500-user license
- J9439A ProCurve Identity Driven Manager 3.0 base product - unlimited user license
- J9440A ProCurve Identity Driven Manager 3.0 additional 1000-user license

This Auto Update pertains to Identity Driven Manager Version 3.0 operating as an add-on module to PCM Plus 3.0.

These release notes include information on the following:

- IDM Notes ([Page 6](#))
- Enhancements ([Page 8](#))
- Software fixes included in the Auto-Update release ([Page 10](#))
- Known issues included in the Auto-Update release ([Page 11](#))

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**.

- ProCurve Identity Driven Manager User's Guide, Version 3.0
- Read Me First for the ProCurve Manager, Version 3.0
- ProCurve Network Management Installation and Getting Started Guide, Version 3.0
- ProCurve Manager Plus Network Administrator's Guide, Version 3.0

© Copyright 2005 - 2009

Hewlett-Packard Development Company, LP.

The information contained herein is subject to change without notice.

Publication Number

5991-4729a
August, 2009

Applicable Products

- J9438A ProCurve Identity Driven Manager 3.0 base product - 500-user license
- J9439A ProCurve Identity Driven Manager 3.0 base product - unlimited user license
- J9440A ProCurve Identity Driven Manager 3.0 additional 1000-user 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.procurve.com

Software Management – IDM 3.0 Update 1


ProCurve Manager 3.0 Update 3 must be installed before installing this ProCurve Identity Driven Manager 3.0 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.

NOTE: If automatic update finds both the PCM 3.0 Update 3 and IDM 3.0 update 1 available for installation, PCM is automatically installed first. If you are manually installing the IDM 3.0 update 1 from the download folder and PCM 3.0 update 3 is not installed, the installation process is halted and a warning message is displayed stating that PCM 3.0 update 3 must be installed first.

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


[Tools->Preferences->Auto Updates for PCM->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 `idm_server_3_0_update_1.zip` file and any applicable IDM Agent files 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.) Possible IDM Agent files for IDM 3.0 Update 1 are:


`IDM_WINDOWS_3_0_update_1.zip`

`IDM_REDHAT_3_0_update_1.zip`

`IDM_SUSE_3_0_update_1.zip`

`IDM_PRONAC_3_0_update_1.zip`

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.

Only new IDM Agents or IDM Agents that have been deployed will be listed with a check 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.

Special Notes

■ Understanding how Update 1 affects IDM Agent Deployment

IDM Update 1 automatically adds IDM Agent support for Windows 2003 64-bit (IAS) and Windows 2008 64-bit (NPS). It also updates the Agent files that exist on the IDM server for any IDM Agents that have been installed from that IDM server. The IDM administrator can control when the IDM server pushes Update 1 to these IDM Agents. However, if a new IDM Agent, such as an IDM Linux Agent, is installed from that IDM server, the IDM Agent deployed will not have been updated to Update 1. This behavior is due to the IDM server not having a deployed IDM Linux Agent at the time the IDM server was updated to Update 1. Therefore, after the Linux Agent deployment, the IDM administrator must Check For Updates again at the IDM server to update the Linux IDM Agent files on the IDM server to Update 1.

■ PR 42058: If PCM 3.0 Update 1 or later is installed but IDM 3.0 Update 1 is not installed, warnings about non-printable characters appear in the IDM Event Viewer.

Workaround: Install IDM Update 1.

■ IDM 3.0 Agent Uninstall – Windows 2003, ProCurve ProNAC 800, and SAIASConnector.ini File

The C:\WINDOWS\SYSTEM32\SAIASConnector.ini file must be manually saved to a backup location before uninstalling the IDM 3.0 Agent on a Windows Server 2003 configured to obtain endpoint integrity status from ProCurve ProNAC 800 devices via the SAIASConnector. Otherwise, NAS IP addresses manually entered in the file must be re-entered after reinstall. New installations are not affected.

Before uninstalling and reinstalling the IDM Agent:

1. Copy the SAIASConnector.ini file to a backup location.
2. Uninstall the IDM Agent.
3. Install the IDM Agent.
4. Replace the new SAIASConnector.ini file with the backed up (original) version.
5. Restart the IAS Services.

■ When using multiple realms, follow these IDM Best Practices:

- No Active Directory synchronization support for realms that the PCM/IDM server machine is not a member of.
- Secondary (non-default) realms require a one-time manual deploy OR 802.1X user login with realm information to associate the IDM Agent/RADIUS server with the realm.

- Clients authenticating from non-default realms must supply the realm name in RADIUS User Name attribute to be correctly auto-discovered (most 802.1X clients provide this attribute). Otherwise, manual configuration of the user in the correct Realm and Access Policy Group is necessary.
- If a realm name has to be changed after AD Synchron or IDM User Import utility to match with 802.1X users, use the following guidelines:
 1. When installing the PCM/IDM server, enter the fully qualified domain name where prompted and use the simple name in the Alias field.
 2. Enable directory synchronization before users start logging in.

To change the Realm name after installation:

1. If no IDM rules have been configured and no users have been manually created, delete the improperly named realm (simple name)
 2. If IDM rules have been configured, delete the new realm that was created when AD Sync ran, rename the original realm with the fully qualified name and set the alias to the short name, then re-run AD Sync
- The IDM Agent Web configuration user interface is not available on ProCurve NAC 800 after changing to a new IDM server. The issue is that the IDM Agent configuration user interface is configured for security purposes to only be accessible from the PCM/IDM server (e.g., you must open a Web browser on the PCM/IDM server to access the IDM Agent Web UI). In short, if the administrator changes the PCM/IDM server in the ProCurve NAC 800's Web UI, the IDM Agent Web UI will no longer be accessible from the original PCM/IDM server and will only be accessible from the new PCM/IDM server.

Enhancements

- New IDM Agent platform support is provided in IDM 3.0 Update 1 for IAS on Windows Server 2003 (64-bit) and NPS on Windows Server 2008 (64-bit).
- PR 14275: When NIM/IDM integration is enabled, NIM mitigation attributes now overlay the existing IDM policy. NIM mitigations can be Rate-Limit, Quarantine to a VLAN, or reject. As an example, if an IDM policy is set to assign a user to a VLAN and the NIM policy is to rate limit the user, the IDM policy will take effect as well as the NIM rate limit. However, if an IDM policy is set to reject a user and the NIM policy is to quarantine or rate limit the user, the IDM reject policy will take precedence.
- IDM Agent now updates the dmagent.dll file for Product Version and File Version.

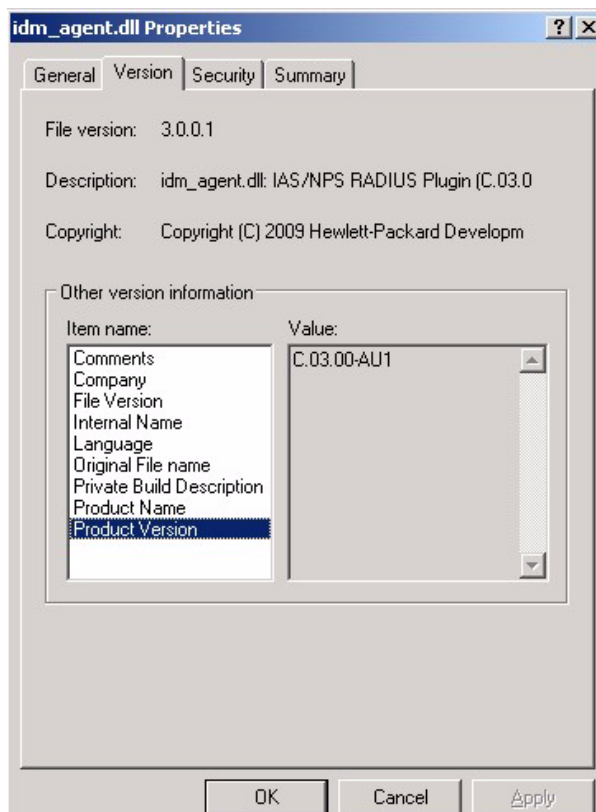


Figure 1. Windows 2003 IAS 64-bit IDM 3.0 AU1 Agent properties

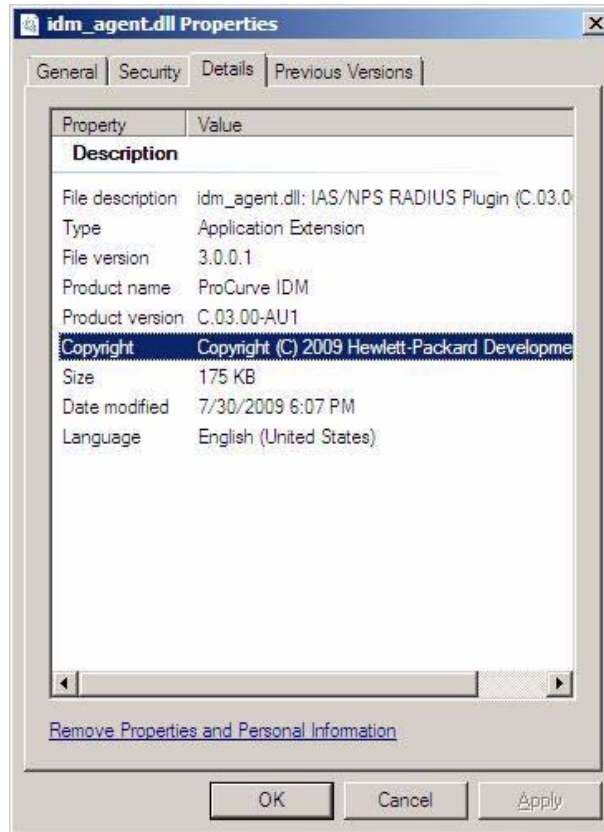


Figure 2. Windows 2008 64-bit IDM 3.0 AU1 Agent properties

Software Fixes in IDM 3.0

Update 1

The following IDM problems were resolved in Identity Driven Manager Update 1:

- PR 41807 and PR 18662: The default Access Policy Group is sometimes incorrectly assigned. The event log shows IDM received an invalid session start event.
- PR 18178 and PR 42955: User global rule modification does not result in automatic deployment of the configuration change to the IDM Agent.
- PR 42146: Certain Access Policy Group names cause automatic configuration deployment to silently fail.
- PR 39254: Active Directory synchronization does not detect all changes to Active Directory when backup domain controller exists.
- PR 17135: The IDM policy is not applied or showing the correct login status when Cisco VoIP phones use 802.1X EAP-MD5 to authenticate with Microsoft IAS.

Workaround: The user must modify IAS request processing by removing the first 9 characters (the model number) from the user name for the Cisco VoIP phones. Once IDM 3.0 Update 1 is installed and the IAS request processing is modified, the login status will be displayed correctly.

- PR 43015: The Session History Details report cannot be generated when the Tagged VLANs column is included.
- PR 39521: IDM server log file IDMImportServer_libadsync.log grows to a very large size if the PCM/IDM server is not restarted at some point. This behavior was changed so that up to four log files are created, each one with a maximum size of 4MB, for a total of 16MB. Utilize the modification date of the files to reconstruct the log.
- PR 42166: The Secure Access Wizard does not proceed past the RADIUS Authentication Servers screen if an IP address is entered for a RADIUS server and an IDM Agent is not installed on the RADIUS server.
- PR 42731: The Secure Access Wizard does not allow for the configuration of WESMzl devices.
- PR 17565: The Secure Access Wizard and the Adding RADIUS Clients Wizard allows non-ProCurve ProNAC 800 FreeRADIUS servers to be selected for adding clients. These RADIUS servers are not supported through these Wizards, and using the Wizards could result in configuration errors.
- PR 17312: The IDM FreeRADIUS Agent installer allows installation to continue when FreeRADIUS was not installed.

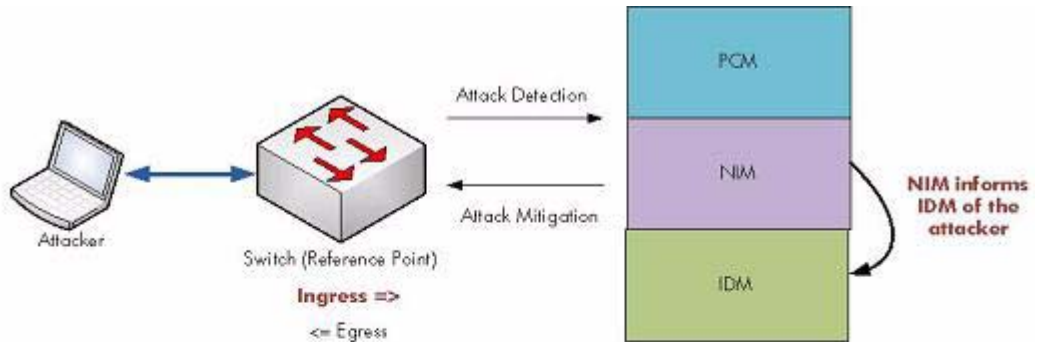
Known Issues in IDM 3.0

Update 1

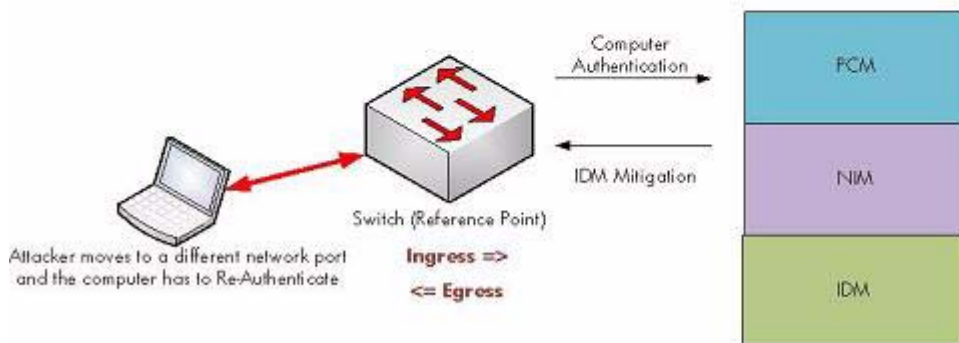
- PR 40822: IDM 3.0 Agent can be installed on unsupported 64-bit OS platforms
Workaround: Uninstall IDM 3.0 Agent and reinstall using the AU1 Agent installer.
- PR 42685 and PR 42952: No warning message is displayed or logged in the IDM event log when the device does not support egress rate limits or tagged VLANs and IDM is attempting to apply those settings to the device.
Workaround: Make sure the devices have support for the functionality IDM is applying.
- PR 43020: The **Start Over** button does not clear values in the "Create a Report" wizard for the Session History Details report.
- PR 42424: Due to limitations in PCM 3.0 Update 3, the Secure Access Wizard cannot configure WESMzl for MAC authentication.
Workaround: Use the WESMzl's Web UI to configure MAC authentication.
- PR 43534: Due to limitations in PCM 3.0 Update 3, no warning message is displayed or logged when unsupported ACLs are configured for ProCurve 28xx switches.
Workaround: Make sure the devices have support for the functionality IDM is applying.
- PR 42208: Due to 6120XG switch limitations, this switch does not start a user session if user's port is statically configured for a tagged VLAN and IDM is configured to provision the user with the same untagged VLAN. Normally, IDM applied values should override any statically configured values on the switch. However, because the tagged VLAN and untagged VLAN are the same value, which is an invalid configuration, an error is recorded before the IDM values override the static values set on the switch.
- PR 42211: Due to switch operations, session start and session end events are displayed up to four times in IDM event log with NPS RADIUS server. There is no workaround.
- Internet Authentication Service (IAS) crash on Windows Server 2003 64-bit: RADIUS service crashes have occurred with C:\Windows\system32\netapi32.dll version 5.2.3790.3959 on Windows Server 2003 64-bit platform. Version 5.2.3790.4392 of netapi32.dll has not been seen to cause this crash. Service Pack 2 is **not** sufficient to avoid this issue. This issue may also appear on other Windows platforms. See <http://support.microsoft.com/kb/958644> for more details.
Workaround: It is recommended to run Windows Update and install the latest high priority updates prior to installing IDM 3.0 Update 1.

Known Issues in IDM 3.0
Update 1

- PR 40474 and PR 14152: Rate-limit action in PCM applies rate-limit ONLY to incoming traffic, PCM should apply it to incoming and outgoing. This behavior is best explained via the following diagram:



When an attack is first detected, NIM applies rate limit mitigation to the Ingress direction on the switch port the Attacker was connected. This behavior is normal for NIM.



When IDM detects the computer authentication and knows that NIM has reported this computer as an attacker, IDM applies rate-limits to both the Ingress and Egress directions of the switch port, which is slightly different than when NIM detects the attack first.

Figure 3. Rate limit Diagram

- Cisco RADIUS clients with older firmware versions (e.g., c3750-ipservicesk9-mz.122-25.SEE3.bin) cannot authenticate users successfully. Newer firmware versions (e.g., c3750-ipservicesk9-mz.122-50.SE.bin and AiroNet AP 1200 with c1200-k9w7-tar.123-8.JEB1.tar) authenticate users with IDM 3.0 and later correctly.

Workaround for the older firmware: If upgrading firmware is undesirable or not an option: Edit C:\Program Files\Hewlett-Packard\PNM\idm-agent\agent\config\DMConfig.prp on the IDM agent\RADIUS server and change send_filter_id=true to send_filter_id=false.

However, if a ProCurve TMSzl module is also a RADIUS client and is configured to use the Filter-ID RADIUS attribute from IDM, making this change will break the TMSzlNDM integration.

