Avocent® Power Management Distribution Unit (PM PDU)
Release Notes
Firmware Version 2.0.1.13
September 14, 2011

This document outlines:
1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug fixes
5. Known Issues
6. Firmware upgrade restrictions on PDUs in chain
7. Recommendations
8. Firmware upgrade for Avocent® PM PDU running V_1.2.0 and older

==
Update Instructions
==

This firmware can be installed over any previous release of the Avocent® Power Management Distribution Unit (PM PDU). The firmware can be updated through either the appliance built-in web interface or the DSView™ 3 management software, which requires the PDU plug-in.

Firmware upgrade may fail due to lack of enough memory to complete the process. This is likely to happen on appliances running on version 2.0.0.20 or older. If the upgrade process fails, it is recommended to release memory and retry the upgrade again before rebooting the unit. To release the memory, please type the following command once logged in as root in the unit: **/etc/init.d/power-display restart**

Please refer to the installer/user guide for detailed instructions on how to update the PDU to this version.

The PDU firmware provides an internal mechanism which preserves existing configuration when upgrading firmware; however, it is strongly recommended that you back-up system configuration before the firmware version is upgraded.

DSView™ 3 software version 3.7.2 (or greater) is required. PDU plug-in version 2.0.1 is recommended.

After PDU firmware has been upgraded to version 2.0.1, it is mandatory to clear the Web browser cache (e.g. press Ctrl F5 in Internet Explorer® or Firefox®) of any system which intends to be connected to the appliance Web interface.

NOTE: The factory default password for **root** is **linux**. The factory default password for **admin** is **avocent.**

==
Appliance Firmware Version Information
==

Appliance Product	Firmware Type	Version	Filename	Part #
Avocent® 3000, 2000 and 1000 PDUs	Opcode	V_2.0.1.13	fl0618-018.bin fl0618-018.bin.md5	FL0618-018

This firmware supports the horizontal and vertical models of the Avocent® 1000, 2000 and 3000 PDU families, which includes units with 3, 6, 10, 20 and 24 outlets.

Other files related to this release are:
- Avocent® PM SNMP MIB: available from a shell session in the PDU at /usr/local/mibs/Avocent-PM-MIB.asn
- Avocent® PM SNMP Trap MIB: available from a shell session in the PDU at /usr/local/mibs/Avocent-PM-TRAP-MIB.asn

NOTE: These files are also available at the Avocent® website at www.avocent.com.

==
Features/Enhancements
==

Please refer to the installer/user guide for details about features supported by the PDU.

The features and enhancements supported by this version of the PDU include:

1. Extended support for SNMP vendor MIB to include setup of power management parameters:

   o   PDU chain (pmPowerMgmtSerialTable): enable/disable buzzer, syslog, SW over-current protection; configuring polling rate and power cycle interval.

   o   PDU table (pmPowerMgmtPDUTable): configuring the PDU ID, setting all levels of current thresholds, resetting its configuration to factory default or rebooting the PDU. Extra information was also included, like alarm status, type of measurement for power, voltage and power-factor, as well as energy info.

   o   Outlets table (pmPowerMgmtOutletsTable): outlet name, post-on and post-off delays and all levels of current thresholds are configurable. Extra information was also included, like alarm status, type of measurement for power, voltage and power-factor, as well as energy info.

   o   Phases and banks (pmPowerMgmtPhasesTable and pmPowerMgmtBanksTable): all levels of current thresholds are configurable. Extra information was also included, like alarm status, type of measurement for power, voltage and power-factor.

   o   Environment sensors (pmPowerMgmtSensorsTable): all levels of thresholds are configurable. Extra information added includes sensors type and alarm status.

   Configuring power management parameters using SNMP are effective upon command completion but they are not saved to flash, thus not persisted through reboots. A new OID (pmPowerMgmtSerialTableSave) was also introduced to save changes done in the PDUs.

   Depending on the PDU model some of the OIDs may not apply. In such case SNMP queries for those OIDs will return 0 (zero) or "N/A" based on its syntax.

   All new and modified OIDs are defined and detailed in the PDU MIB file.

2. Support configuration via bootp request. The Bootp Configuration Retrieval option allows the entire unit configuration to be retrieved over Bootp/TFTP during boot and during DHCP renewal.
   There are two ways to push a configuration during a DHCP request/renewal. The configuration can be sent as file created by the Save Configuration appliance system tool, or it can be sent as a CLI script to be executed under the command line scripting interface. When using the CLI approach, it is recommended to create the file by executing the list_configuration command only over the specific nodes that are affected.
   Although this feature is enabled by default it requires the saved configuration file to be available in a TFTP server as well as changes in the DHCP server configuration to trigger the file transfer.

3. OpenSSL upgrade from version 0.9.8k to 0.9.8q, which includes fixes for the following security issues: CVE-2010-4180, CVE-2010-4252, CVE-2010-3864, CVE-2010-2939, CVE-2010-0742, CVE-2010-0740, CVE-2010-0433, CVE-2009-3245, CVE-2009-4355, CVE-2009-1378, CVE-2009-1377, CVE-2009-1379, CVE-2009-3555

4. Apache upgrade from version 2.2.9 to version 2.2.17 because of the following security issues: CVE-2010-1452, CVE-2010-0408, CVE-2010-0425, CVE-2010-0434, CVE-2009-3555, CVE-2009-2699, CVE-2009-3095, CVE-2009-3094, CVE-2009-2412, CVE-2009-1891, CVE-2009-1195, CVE-2009-1890, CVE-2009-1191, CVE-2009-0023, CVE-2009-1955, CVE-2009-1956, CVE-2008-2939.

===
Bug fixes
===

Firmware version 2.0.1.13
- 67635 (L3 65643588): Set SNMP SysObjectID correctly upon firmware upgrade.
- 67680 (L3 65616124): Prevent from stopping transmission in chained PDUs. When receiving corrupted characters, the PDU may go offline, but will resume communication shortly.
- 67764: Add bootpconf file when saving configuration.
- 67765: Security issue CVE-2011-3192.

Firmware version 2.0.1.11
- 66866: Support for IE-9 and Firefox 5.
- 66955: Resource leakage in daisy chain PDUs.
- Security patches: CVE-2011-0726, CVE-2011-1171, CVE-2011-1172, CVE-2011-1182, CVE-2011-1593

Firmware version 2.0.1.8
- Fix resource allocation in outlet driver.
- 65679: Apply last saved outlet status and post-on delays when unit is turned on (cold start).
- 65737: Display appliance serial number in DSView™ Unit page. It requires deleting and re-adding the PDU in the DSView™ .

Firmware version 2.0.1.5
- 62596: Telnet, SNMP and NTP could not restart after restoring configuration.
- 63615: Configuration of date and time issues that caused the display of warning message "The date and time specified is outside of the DSView™ . DSView™ 3 will not able to manage this appliance"
- 62899: The SNMP answer for sysObjectId is the Product Object ID.
- 64068: Confirmation message to turn on/off outlets refers to individual outlet rather than the entire PDU.
- 58209: Extended expiration date of the appliance viewer applet certificate.

===
Known Issues
===

This release contains the following known issues:

- 57435: Outlet status remains ON in case of a blown fuse in the bank that the outlet belongs to. The blown fuse indication shows only in the bank level.
- 57437: The unit is unable to provide values for the bank B and its outlets when a blown fuse happens in bank A of a PDU, thereafter showing N/A for the measurements in that bank.
- 55876: Due to internal value conversions, configuring thresholds for temperature environment sensors may result in a slightly different value compared to the configured value
- 55667: During firmware upgrade of any PDU in chain, the serial port (out/aux) will be exclusively allocated to that process, and no PDU in the chain will accept commands. Due to the size of the firmware and the time required to transfer the file through the serial port, chained PDUs will not be

shown in for the PDU list as long as the process lasts. There is no indication that the PDU in the chain is being upgraded or when the process finishes.

- 57369: In some cases, upgrading the firmware of a Cyclades™ Intelligent Power Distribution Unit (IPDU) will cause the entire chain to momentarily disappear. The chain is automatically rediscovered when the firmware upgrade process is completed.
- 55691/55739/55740/55743: Configuration or operation in long chains may delay up to a few minutes to complete.
- 57093: Changing the configuration of a chained PDU may show a message about a connection lost to the PDU. The communication is automatically resumed after a few seconds.
- Detection of Cyclades™ IPDUs with 2-segment running firmware version 1.9.1 will fail if the unit is daisy chained after a Cyclades™ IPDU running firmware version 1.9.2.

===
Firmware upgrade restrictions on PDUs in chain
===

All PDUs in the chain must be running at least version 2.0.0 to allow for firmware upgrade via serial port.

Upgrading the PM PDU firmware when the unit is connected to the serial port of a console server is also possible for the following products and versions:

ACS 6000 advanced console server version 2.2.0 or newer.

ACS 5000 advanced console server version 3.3.0 or newer.

ACS advanced console server version 3.3.0 or newer.

Upgrade scenarios, assuming PDUs running version 1.3.0 or older:

1. One PDU (1000, 2000 or 3000 PDU) connected directly to the Ethernet network, with or without multiple Cyclades™ IPDUs (42, 10, 10i, 20, or 20i IPDUs, and so on) chained to it; this scenario supports firmware upgrade on all the PDUs.
2. One PDU (1000, 2000 or 3000 PDU) connected directly to the Ethernet, with one or more PDUs chained to it; this scenario only supports firmware upgrade on the PDU that is directly connected to the Ethernet.
3. One console server or DSR™ KVM over IP switch with one or more PDUs (1000, 2000 or 3000 PDU) chained to it; this scenario does not support firmware upgrade on the PDUs.

===
Recommendations
===

- It is strongly recommended that all Avocent™ PDUs in a chain are upgraded to this released version.
- It is strongly recommended that all Cyclades™ IPDUs in a chain are upgraded to version 1.9.2

- In a PDU chain of mixed types, in order to minimize traffic on the chain serial connections, it is more effective to put the appliances with a higher number of outlets at the top of chain. For example, units with 24 or 20 outlets should be placed before units with 10, 6 or 3 outlets.

==
Firmware upgrade for Avocent™ PDU running version **1.2.0** and older
==

This special procedure is only required for firmware upgrade of PDU running version 1.2.0 and older.

Please make sure the PDU is connected to the network before starting the upgrade process.

Do not use DSView™ 3 software to perform the upgrade. Instead, perform the upgrade using the unit web interface but do not reboot when it finishes, even if the result shows success.

Once the upgrade is successfully done, login to the unit as root and run the following steps:

[root@MyPM ~]# /sbin/checkBoot /tmp/avoImage > /tmp/uboot.zip

Checksum must return OK.

[root@MyPM ~]# gunzip -c /tmp/uboot.zip > /tmp/uboot

Return no errors

[root@MyPM ~]# cat /tmp/uboot > /dev/mtdblock7

Return no errors

Do not reboot the appliance if any of the steps above return error. In such case, you can repeat the steps above, or start over the entire upgrade process from web interface by removing the files created:

[root@MyPM ~]# rm -f /tmp/avo* /tmp/uboot*

Firmware upgrade from version1.2.0 and older requires a CPU reset (button located in the front panel), that demands physical access to the unit. Please follow these steps to restart the unit after firmware upgrade.

NOTE: Follow these steps only after the firmware is downloaded and installed. Otherwise, the appliance console will not work properly due to a mismatch on the port speed, preventing the unit from working in a chain.

a. Login to the appliance's console as root user.

b. Type "shell" in case the cli prompt shows upon login:
   --:- units cli-> shell

   WARNING: Improper use of shell commands could lead to data loss,
   the deletion of important system files or other unexpected result.
   Please double-check your syntax when typing shell commands.

   [root@PM1024-1234567890 ~]#

c. From shell prompt, execute shutdown command:
   [root@PM1024-1234567890 ~]# shutdown -h now

   Broadcast message from root (pts/0) (Thu Mar 5 20:33:45 2009):

```
The system is going down for system halt NOW!
[root@PM1024-1234567890 ~]# Power down.
System Halted, OK to turn off power
```

d. Once the system is halted, use a paper clip to press the CPU reset button located in the front panel in the appliance. Wait a few seconds after reset for visual feedback from the LED display.