Avocent® Power Management Distribution Unit (PM PDU)
Firmware Release Notes
Version 2.0.1.23
July 13, 2015 UPDATE!

This document outlines:

1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug Fixes
5. Known Issues
6. Firmware Upgrade Restrictions (PDUs in the chain)
7. Recommendations

==========

1. Update Instructions

==========

ATTENTION: This firmware version should not be loaded into the following models:

PM3003H-401 and PM2003H-401 PDUs

PM3003V-401 and PM2003V-401 PDUs

PM1005V-401 PDU

NOTE: These PM PDU models require firmware version 2.1.0.23.

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 Avocent® DSView™ management software, which requires the PDU plug-in.

NOTE: It is recommended that DSView™ 4 users upgraded the PM PDU plug-in to version 2.0.1.7.

NOTE: 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.

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, enter the following command once logged in as root in the unit: **/etc/init.d/power-display restart**.

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

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

After PDU firmware has been upgraded to version 2.0.1.23, it is mandatory to clear the Web browser cache (such as by pressing **Ctrl F5** in Internet Explorer or Firefox) of any system which intends to be connected to the appliance Web interface.

==========

2. Appliance Firmware Version Information

==========

Appliance Product	Firmware Type	Version	Filename
Avocent® 3000, 2000 and 1000 PM PDUs	Opcode	V_2.0.1.23	zImage_pmhd_2.0.1.23.bin zImage_pmhd_2.0.1.23.bin.md5

This firmware supports the following models: PM3003H-401 and PM2003H-401 PDUs, PM3003V-401 and PM2003V-401 PDUs and the PM1005V-401 PDU.

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.

==========

3. Features/Enhancements

==========

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

The features and enhancements supported by PDU version 2.0.1.23 include:

- OpenSSL upgraded to address the POODLE issue.
- Configuration changes as a result of this release are in the Security Profile menu, Enable HTTPS drop down list:
    - SSL version 2 and 3 have been replaced with TLS versions 1.0, 1.1 and 1.2
    - Configurations that were HTTPS SSL3 in the previous release will be upgraded to TLS1.2. All other configurations in the previous release that had SSL2 will be upgraded to TLS1.1, TLS1.2 + TLS1.

The previous version (2.1.0.22) shows the maximum current of the PDU for international models. The features and enhancements supported by PDU version 2.0.1.22 include:

- Upgraded Bash to address the Shell Shock issue.

The features and enhancements supported by the previous PDU versions include:

- Extended support for SNMP vendor MIB to include setup of power management parameters:
    - PDU chain (pmPowerMgmtSerialTable): enable/disable buzzer, syslog, SW over-current protection; configuring polling rate and power cycle interval.
    - 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.
    - 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.
    - 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.
    - 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.

- 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.
- OpenSSL upgrade
- Apache upgrade from version 2.2.9 to version 2.2.17

==========

4. Bug Fixes

==========

NONE

==========

5. 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.

==========

6. Firmware Upgrade Restrictions (PDUs in the 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:

- Avocent® ACS 6000 advanced console server version 2.2.0 or newer.
- Avocent® ACS 5000 advanced console server version 3.3.0 or newer.

- Avocent® ACS advanced console server version 3.3.0 or newer.

Upgrade scenarios, assuming PDUs running version 1.3.0 or older:

- One PM PDU (PM 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.
- One PM PDU (PM 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.

One console server or DSR™ KVM over IP switch with one or more PM PDUs (PM 1000, 2000 or 3000 PDU) chained to it; this scenario does not support firmware upgrade on the PDUs.

==========

7. Recommendations

==========

- It is strongly recommended that all Avocent® PM 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.