Avocent® ACS 6000 Advanced Console Server
Release Notes
Version 3.0.0.12
October 24, 2014

This document outlines:

1. Update Instructions

2. Appliance Firmware Version Information

3. Features/Enhancements

4. Bug Fixes

==========

1. Update Instructions

==========

NOTE: Please refer to the ACS 6000 Installation/Administration/User Guide for detailed instructions on updating the ACS 6000 console server to version 3.0.0.

IMPORTANT NOTE: **This version should be upgraded from version 2.5.0-11. Appliances with earlier versions should be upgraded to version 2.5.0-11 before the upgrade to version 3.0.0.12.**

In order to have all features listed in this release available through DSView™ management software, DSView™ software version 4.1.0.141 or later and ACS 6000 console server plug-in version 3.0.0.6 are required.

After the ACS 6000 console server firmware has been upgraded to version 3.0.0, it is mandatory that the web browser cache of any system which intends to be connected to the ACS 6000 console server web interface is cleared. To do this, press **Ctrl-F5** from the browser.

ACS 6000 console server firmware version 3.0.0 provides an internal mechanism which preserves the existing configuration when upgrading from firmware version 2.5.0. However, it is strongly recommended that you back up the system configuration before the firmware version upgrade.

==========

2. Appliance Firmware Version Information

==========

Appliance/Product	Firmware Type	Version	Filename	Part #
Avocent® Cyclades™ ACS 6000 Console Server	Opcode	V_3.0.0.12	FL0585-035.bin FL0585-035.bin.md5	FL0585-035

==========

3. Features/Enhancements

==========

NOTE: Please refer to the ACS 6000 Installation/Administration/User Guide and/or Command Reference Guide for details about features supported by the ACS 6000 console server version 3.0.0.

Client Browser Support Information:

- Microsoft Internet Explorer 8 or 9

- IE-9 may require you to click *Refresh* in the top-right of the frame to refresh the content of the page when a *Request in Progress* message appears and stays.
- IE-8 may not work for an HTTPS session.

- Mozilla Firefox version 16.0.2 in Mac OS X 10.7.4, version 17.0.1 in Windows 7.
- Safari version 6.1.3 in Mac OS X 10.7.4.
- Google Chrome version 23.0.127197m in Windows 7.

Upgrade included in ACS 6000 console server version 3.0.12:

- Bash version 4.2.53 that has fixes for the following: CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278

Upgrades included:

- Linux Kernel version 3.12.1

  NOTE: The support for PCMCIA cards that are supported by previous firmware versions are affected by this upgrade. The card may not be detected in this release.
- OpenSSL version 1.0.1h
- Apache version 2.2.27
- OpenSSH version 6.6p1
- OpenLdap version 2.4.29
- Syslog-ng version 3.5.4
- OpenSwan 2.6.41

Major features of the ACS 6000 console server version 3.0.0.11 include:

- Renew IP address on link down/up event. It will send DHCP renew request on link down/up event detected by Linux Kernel in network interfaces.
- Support fourth Generation Wireless Modem:
  - Devices
    - Huawei – model E368 USB Connect Force 4G
    - ZTE – model MF662 USB Modem (APAC - 21.6Mbps)
  - Profiles: network (wwan0 interface) or dial-in/dial-out (Huawei - ttyUSB0 and ZTE – ttyUSB2)
  - WWAN Profiles: always ON, schedule connect/disconnect or manual ON/OFF

  NOTE: When DHCPv4 fails to get the IPv4 address, it may require a reset of the wireless modem. There are two ways to reset the wireless modem:
  - Hard Reset: Physically unplug and then plug the device back in.
  - Soft Reset: Equivalent to hard reset, this can be achieved without removing the modem by switching from an Enable to Disable status in network (wan) mode.

  NOTE: These devices do not support IPv6.

  NOTE: The following information is required for the wwan to work properly:

- APN: Should be verified with the service provider. For example, APN for AT&T is ‘broadband’.
- PIN: If locked, SIM is used. Multiple incorrect attempts with PIN may result locking the SIM. PIN is not needed when unlocked SIM is used.

- Emerson Network Power MPH2 appliances as well as MPX/MPH units with RPC2 cards installed are supported via serial port. The following actions are supported:
  - Auto-detect in serial ports with power profile: vendor ENP (Emerson Network Power)
  - Management PDU
    - View information: vendor, model, firmware version, and number of outlets, of circuits and of phase.
    - Rename PDU
    - Power Control (On/Off/Cycle)
    - Reboot
    - Factory Default
  - Management Outlets
    - Rename Outlets
    - Set Post-On and Post-Off delays
    - Power Control (On/Off/Cycle/Lock/Unlock)
  - Power Measurement
    - Collect measurements: current, power consumption, power factor, voltage, accumulated energy.
    - Set current thresholds
  - Environment Sensors
    - View Temperature and Humidity sensors measurements
    - Set thresholds for Temperature and for Humidity sensors
    - View state of dry contacts and digital ports
- Emerson Network Power MPH2 appliance as well as MPX/MPH units with RPC2 cards installed and Avocent Power Management Power Distribution Units (PDUs) are partially supported via network using SNMP commands. The support is restricted to the following actions:
  - Get status of the outlets
  - Power control outlets (turn on, turn off, cycle)
  - Rename outlets
  - Rename PDU
  - Allow merge the outlets to targets.

  Each ACS 6000 console server can support a maximum number of 48 PDUs via SNMP.
- Enhancements in Security Profile:
  - SSH allows authentication via username/password (Challenge Response Authentication is enabled)
  - SSH minimum cipher and mac level: low and high.
    - Low: allow all ciphers and macs supported by SSH

        - High: allow only ciphers: aes128-ctr, aes192-ctr, aes256-ctr, arcfour-128 and arcfour-256; and only macs: RIPE_MD-160 and umac-64
    - SSH minimum cipher and mac level is high in Secure Profile
- ACS 6000 console server serial viewer is updated to comply with Java 5 update 71 security level HIGH.
- ACS 6000 console server can be connected to Fiber Optic Network via Avocent “Converter for Multimode Fiber” (FMCMMGB-001)

==========

4. Bug Fixes

==========

Bug fixes include:

- Target Names updated in appliance will be pulled to the DSView™ management software by the DSView software auto-pull name feature (L3-487234-326093733)