Avocent® ACS 6000 Advanced Console Server
Release Notes
Version 2.5.0.2
January 17, 2013

This document outlines:

1. Update Instructions
2. Appliance Firmware Version Information
3. Features/Enhancements
4. Bug Fixes
5. Known Issues

==========

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 2.5.0.

In order to have all features listed in this release available through DSView™ management software, DSView™ software version 3.7.1 or later and ACS 6000 console server plug-in version 2.5.0.1 are required.

After the ACS 6000 console server firmware has been upgraded to version 2.5.0, 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 2.5.0 provides an internal mechanism which preserves the existing configuration when upgrading from firmware version 2.4.0. 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_2.5.0.2	FL0585-026.bin FL0585-026.bin.md5	FL0585-026

==========

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 2.5.0.

Client Browser Support Information:

- Microsoft Internet Explorer 8 or 9
- Mozilla Firefox version 16.0.2 in Mac OS X 10.7.4, version 17.0.1 in Windows 7.
- Safari version 5.1.7 in Mac OS X 10.7.4.

- Google Chrome version 23.0.127197m in Windows 7.

Upgrades included:

- OpenSSL version 0.9.8x has fixes for security issues: CVE-2012-1165, CVE-2012-2333, CVE-2012-2110, CVE-2012-2131, CVE-2012-0884
- Apache version 2.2.23 has fixes for security issues: CVE-2012-0883, CVE-2012-2687.
- OpenSSH version has fixes for security issues: CVE-2010-4478, CVE-2012-0814, CVE-2011-0539

Major features of the ACS 6000 console server version 2.5.0 include:

- Liebert® MPH™/MPX™ PDUs and ServerTech 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 ACS6000 console switch can support a maximum number of 48 PDUs via SNMP.
- X.509 Certificates for HTTPS connections can be generated (self-signed) or be downloaded to the appliance via OBWI, CLI and DSView/Plug-in.
- SNMPTrap Proxy allows administrator to configure the appliance to send received snmptrap messages to a remote Network Management System.
- Dial-Out On-Demand allows administrators to configure serial port, internal modem or pluggable modem to establish PPP link over dial-out connection when needed.
- Socket Client profile for serial ports allows administrator to connect a device that does not have network interface to sever via socket tunnel.
- CAS profile supports all combinations of the protocols Telnet, SSH and Raw Mode to access the target connected to the serial port. Each protocol has its own specific TCP port alias.
- Local and NFS Data Buffering files can be rotated every day based in time.
- Each alert string can be associated to shell script that will be called when there is a match.
- License is no longer required by ACS 6000 to manage ServerTech PDUs.
- Remote Syslog as destination for events allows administrator to configure the TCP port to be used to send the syslog message.
- The map of DSView™ Establish Viewer Session Right to ACS 6000 Session Target Access Rights is configurable. Default map: Multiple Read/Write access, kill multi-session and send message to multi-session.
- The Appliance Access Right allows administrator to give the Disconnect Session Right to a group without giving the right to reboot the appliance.
- Search list for host-name lookup is configurable when environment has multiple domains for Internet Domain Name System (DNS).
- CLI/wiz allows administrator to enable/disable IPv6 support.
- Support the fwset command as ACS classic supports.

- Improved performance to establish sessions with targets connected to the serial ports.
- Monitoring Serial Ports allows administrator to reset the statics counters of serial ports.

==========

4. Bug Fixes

==========

Bug fixes include:

- Break Sequence in SSH session will generate a break in the serial port when it comes as the first characters in the line. (L3-65695777)
- Apache upgraded to version 2.2.23 to fix security issues (L3-65695732)
- Apache configuration file was updated due security issues with ETag. (L3-65696138).
- OpenSSH upgraded to version 6.1p1 to fix security issues (L3-65696138).

==========

5. Known Issues

==========

This release contains the following known issues:

- The DSView™ software authentication type does not work when the FIPS module is enabled.
- Firmware Upgrade for a PDU under the Power Management- PDU node has the following restrictions:
    - Multi-selection is available only for PM x000 PDU family
    - May return error when more than one PDU is selected for the operation. In this case, click in the Power Management- PDU node in the left menu. The status of a PDU will show up as *Not Available*. Wait, and then click in the node again. When the status changes to *Online*, select the PDU again and click *Reboot* (the PDU requires a reboot after firmware upgrade).
- Wireless LAN devices (PCMCIA cards 16/32 bits and USB) are not supported.
- NIS, IPSec and NFS data logging are supported over IPv4 only.
- The outlet table under the PDU Devices drill-down menu in the web interface is not automatically refreshed after a cycle action for SPC power devices and Server Technology PDUs. The user needs to click the *Refresh* button.
- Changes in configuration related to session (including Idle Timeout and Appliance Session Data Logging) are only effective in the next login.
- To use keys in SSH sessions, the authentication type should be configured as local.
- In a CAS profile, the options for Auto Discovery and Auto Answer are mutually exclusive. Both cannot be enabled in the CAS Profile configuration for one port. If *Auto Answer* is selected in the Serial Port 1, Auto Discovery cannot be configured in the Serial Port 1, because both features work with probes and matches, though in a different way.
    - Auto Answer tries to match the input. When it matches, it sends the output string
    - Auto Discovery sends the probe string and waits for the input to match with the match string that will handle the target name.
- For SPC power devices and Server Technology PDUs, the maximum value for a polling interval is 20 seconds.
- The paste configuration generated by the list_configuration command should not have more than 80477 characters.

- The PPP configuration through the OBWI and CLI in the Dial-In pages is failing in the first time. This requires a re-configuration of the PPP fields.
- The PM PDU firmware version 1.9.2 does not recognize the currseg command. A chain of PDUs that has two segments/circuits should have the same version (for example: all PM PDUs with v 1.9.2 or all PM PDUs with v 1.9.1).
- The Event # 308 – PDU Firmware Upgrade Result will not be generated when the PDU is an Avocent® Power Management Power Distribution Unit (PM PDU).
- The OTP Auto Refresh operation in the DSView™ 3 software is failing to restart the sequence number for the OTP user. The customer should log in to the appliance using “root” user and run the **opiepasswd –c <username>** command, and type the passphrase as asked for.