Avocent® ACS 6000 Advanced Console Server
Release Notes
Version 2.5.0.12
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 2.5.0.

NEW! This patch release is required to update ACS 6000 console server firmware from version 2.5.0-10 or earlier to version 3.0.0-11 or later. 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 2.5.0.5 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_2.5.0.12	FL0585-036.bin FL0585-036.bin.md5	FL0585-036

==========

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.

Upgrade included in ACS 6000 console server version 2.5.0.12:

- 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:

- 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 6.1p1 has fixes for security issues: CVE-2010-4478, CVE-2012-0814, CVE-2011-0539

Major features of the ACS 6000 console sever version 2.5.0.5 include:

- Local Accounts Lockout disables a user account if authentication fails more than configured number. Administrators can configure the following parameters under *User- Local Accounts- Password Rules*:
    - Number of Permitted Failed Attempts
    - Account lockout duration after each fail
    - Unlock account after:
        - value greater than 0 - automatic unlock the account after minutes locked.
        - 0 – locked accounts require manual unlock

  Administrators can manually unlock accounts from the *User-Local Accounts-User Names* page. The table show the number of failed authentication for each account.
- Administrators can configure the port access rigths for all user when it is not controlled by authorizations assigned to user groups.

  The new configuration is under *System-Security- Security Profile*:
    - Port Access
        - Controlled by authorizations assigned to user groups
        - Apply to All Users
            - Session
                - Single Session R/W
                - Multiple Session R/W
            - Kill Multi Session
            - Send Message Multi Session
            - Power Control
            - Darta Buffer Management

  The CLI command to configure the port access is updated; the old command is not valid.

Major features of the ACS 6000 console server version 2.5.0.2 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 ACS 6000 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 software/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 the ACS 6000 console server 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.
- Supports the fwset command as the ACS console server legacy models support.
- 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

==========

Patch release version 2.5.0.10 bug fixes include:

- Updating the PPP authentication from CHAP to PAP will work without exceptions (L3-487234-299514766).

- Default value for initchat in dial-in profile does the reset of the modem (L3 487234-360224706 and L3 487234-377750934)
- The DSView™ software appliance replacement will update the unit configuration as expected (L3-487234-309931712)
- DSView_down_local authentication will fall back to local when the DSView™ software server is not available (L3-65726089)
- The use of debug tools in serial targets via telnet connection will work (L3-487234-347021891)

Patch release version 2.5.0.7 bug fixes include:

- Closing access session to target will proceed normally without exceptions. (L3-65710133, L3-65720695, L3-65719050 and L3-65721152).
- Authentication Type TacacsDownLocal will work as early versions (L3-65717210).
- User authenticated by Tacacs+ server will have the user profile defined by Tacacs Level when it is configured. (L3-65712785).
- Firmware upgrade from the DSView™ software will work from this version 2.5.0.7 on.
  NOTE: The firmware upgrade from the DSView™ software will not work for appliances with version 2.5.0.2 and 2.5.0.5. In these cases, a customer should perform a firmware upgrade via OBWI (L3-65722955).
- The Status of the target in the DSView™ software Topology page will be In Use when there is at least one session opened against the target/port (L3-65721338).

Patch release version 2.5.0.5 bug fixes include:

- Files created by Data Buffering in the NFS server will have permission: Owner-R/W, Group-R and Other-R. (L3-65709655 and L3-65706633).
- Weak Diffie-Hellman will not be allowed in HTTPS sessions.
- Permission of files that have plain-text password/secret will be updated to be readable only by its owner.
- PPP authentication by remote peer in the dial-in and in the dial-out configuration includes correct parameters in the pppd configuration.

Version 2.5.0.2 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).