Avocent® ACS 6000 Advanced Console Server
Release Notes, Version 2.4.0.19
June 8, 2012

This document outlines:
1. Update Instructions
2. Appliance Firmware Version and Language Support Information
3. Features/Enhancements
4. Bug Fixes
5. Known Issues

==========

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 2.4.0.

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 2.4.0.3 are required.

After the ACS 6000 console server firmware has been upgraded to version 2.4.0, 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 2.4.0 provides an internal mechanism which preserves the existing configuration when upgrading from firmware version 2.2.0. However, it is strongly recommended that you back up the system configuration before the firmware version is upgraded.

==========

Appliance Firmware Version and Language Support Information

==========

Appliance/Product	Firmware Type	Version	Filename	Part #
Avocent® Cyclades™ ACS 6000 Console Server	Opcode	V_2.4.0.19	FL0585-022.bin FL0585-022.bin.md5	FL0585-022

==========

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 2.4.0.

Major features of the ACS 6000 console sever version 2.4.0.19 include:

- Support DSView™ software version 4.
- OpenSSL upgrade from version 0.9.8t to 0.9.8x because of the following security issues: CVE-2012-1165, CVE-2012-2333, CVE-2012-2110, CVE-2012-2131, CVE-2012-0884

Major features of the ACS 6000 console sever version 2.4.0.17 include:

- Apache™ upgrade from version 2.2.20 to 2.2.22 because of the following security issues: CVE-2011-3192, CVE-2012-0021,CVE-2012-0031 and CVE-2012-0053
- OpenSSL upgrade from version 0.9.8r to 0.9.8t because of the following security issues: CVE-2011-4108, CVE-2011-4109, CVE-2011-4576, CVE-2011-4577, CVE-2011-4619 and CVE-2012-0027
- Kerberos – applied patch to fix security issue: CVE-2011-4862.

Major features of the ACS 6000 console sever version 2.4.0.12 include:

- A standalone ACS 6000 console server will not require a power device license to manage the Server Technology Sentry™ family of Switched Cabinet Power Distribution Units (CDUs), Smart Cabinet Power Distribution Units (Smart CDUs), switched CDU Expansion Module (CW/CX), Power Tower XL™ (PTXL) and Power Tower Expansion Module (PTXM) power devices.

Major features of the ACS 6000 console sever version 2.4.0.11 include:

- Apache upgrade from version 2.2.17 to version 2.2.20 because of the following security issues: CVE-2011-0419 and CVE-2011-3192.

Major features of the ACS 6000 console server version 2.4.0 include:

- The ACS 6000 console server uses an embedded FIPS 140-2-validated cryptographic module (Certificate #1051) running on a Linux® Power PPC platform per FIPS 140-2 Implementation Guidance section G.5 guidelines.
    - A customer can enable or disable the FIPS module via the OBWI or CLI. With every update, the appliance will reboot and the SSH keys will be re-generated.
    - The following applications will be in FIPS mode of operation when FIPS module is enabled: HTTPS, SSHv2, SNMPv3 and ADSAP2.
    - The time period to boot up the appliance will be longer when the FIPS module is enabled because of the power-up self test (it takes almost 10 minutes).
    - The time period to establish an SSH session will be longer when the FIPS module is enabled because of the verification of the integrity of the cryptographic module.
- Web user interface usability enhancements:
    - My Computer: new option to transfer a file from/to the appliance to/from the computer where the browser is running. The option is available for the following operations: Save Configuration, Restore Configuration, Upgrade Firmware and Power Management – Upgrade Firmware.
    - Make sure the browser allows you to store a file in the computer for the Save Configuration operation.
- Event Notifications: There are new events when the FIPS module is enabled:
    - Event 16 – FIPS compatible OpenSSL self test failed
    - Event 17 – Service in FIPS mode
    - Event 18 – Service in non-FIPS mode
- Login Banner support:
    - The administrator can enable and configure the login banner via the OBWI and CLI.
    - The login banner is supported by the following sessions: Telnet, SSHv2, OBWI and console.
- Group authorization: There is now a new session idle timeout attribute:
    - If the group authorization that the user belongs to does not have the session idle timeout configured, the appliance session idle timeout will be applied for the session. (Available in patch release v 2.2.0-19.)
- 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. (Available in patch release v 2.2.0-19)
- Feature Alert Strings:
    - Supports regular expression in the configuration of the string. (Available in patch release v 2.2.0-19.)
- Multiple Routing Tables: This feature is supported:
    - This feature allows a customer to configure different networks by built-in Ethernet interface (ETH0 and ETH1) and to have one default gateway for each interface. This feature works only for IPv4 network and requires static configuration of the IP address in both interfaces. (Available in patch release v 2.2.0-19.)

==========

Bug Fixes

==========

Patch release v 2.4.0.19 bug fixes include:

- Security issues in OpenSSL are fixed (see Feature/Enhancements) (L3-65673035).
- OBWI and CLI accept a control character in the configuration of CLI command in the Login Profile configuration (L3-65674591).
- OBWI and CLI accept dot (‘.’) as part of the hostname in Appliance Name configuration. This name will be sent as part of the log message to remote syslog servers.(L3-65672468)

Patch release v 2.4.0.17 bug fixes include:

- Customized time zone is stored during the Save Configuration command to be restored via the Restore Configuration feature. (L3-65642054).
- Telnet session to the serial port does not translate CR to LF. (L3-65645567)
- /etc/shadow file is readable only by root user. (L3-65640351).
- Multi-session feature: Data traffic to sessions does not stop when there is at least one session able to receive data from the serial port.
- CLI allows customer to type **Login Banner** with multiple lines using the following instructions: Type the text between double quotes and enter new line as \\n (double back-slash plus character 'n'). (L3-65660471).
- Security issues in Apache, OpenSSL and Kerberos are fixed (see Feature/Enhancements). (L3-65662941, L3-65666162, L3-65666512).
- Tacacs+ accepts pound character ('#') as part of the secret key. (L3-65654553).

Patch release v 2.4.0.11 bug fixes include:

- The following files have new Linux® permissions (L3-65640351):
  - /etc/shadow: read only root user
  - /etc/passwd: read/write only root user
  - /etc/groups: read/write only root user
- OBWI and CLI accept a control character in the configuration of options for the ts_menu in the Login Profile configuration (L3-65640514). (See next bullet for control character explanation.)
- The appliance allows a customer to use a control character to send a break to the serial port during a session against the serial port, when the Break Sequence is configured with a valid control character. A valid control character is a string with two characters: the caret ('^') is the first one, followed by a letter or one of the following special characters: square bracket ('[','] '), backslash ('\'), caret ('^') , underscore ('_'). (L3-65628203).
- The IP alias and TCP port alias of the serial port are not available in the appliance when the status of the serial port is configured as disabled.

Patch release v 2.4.0.9 bug fixes include:

- Bonding activates primary interface (ETH0) during fallback operation. (L3-65627546)
- The IP alias of the serial ports does not affect the remote session to the appliance (ssh/telnet session against appliance). (L3 65622292)
- The Enterprise OID is the ACS 6000 console server family OID (Enterprises.10418.16) in the SNMPTRAP message and in the ACS6000-TRAP-MIB.asn file. (L3 65614727)
- The Serial Viewer uses the SSH port configured in the Security Profile. (L3 65623184)
- A login of the root user in the appliance's console port will perform authentication using the configured appliance authentication type. An ACS 6000 console server allows an administrator to enable fallback locally, only for the root user in the appliance's console port. The configuration is available on the Appliance Authentication page (by default it is disabled). (L3 65627586)
- The OBWI works with Internet Explorer® 9 and Firefox® 5 clients.
- The production script now correctly reports Ethernet test results.
- Saveconf and restoreconf commands have the option to transfer a configuration file to/from TFTP server. (L3 65630647)
- Wiz command in CLI shows the default gateway configured via OBWI/CLI when the method is configured as static. (L3 65634438)
- The restoreconf command restores serial ports configuration between appliances with different number of serial ports. (L3 65634439)

Other bug fixes include:

- Telnet Send Break command sends the break signal to the target device. (L3 65582372).
- In the CLI, the –C option allows a customer to execute a CLI command in no-interactive mode. (L3-65589589).
- The SNMP community name now supports special characters. (L3-65602362).
- The SNMP answer for sysObjectId is the Product Object ID.
- The logging configuration depends on the configuration of Data Buffering, such as, the logging configuration will be effective only if the Data Buffering status is configured as 'enabled'. (L3-65605084).

- The syslog message header shows only the host name of the appliance. (The string 'src_dev_log@' was removed from the syslog message).
- The CPU info now shows the correct processor name: 440EPX.
- The ACS 6000 console server supports a chain of PM 10/20/30A PDUs with version 1.9.1.
- Minimum value for Session Idle Timeout is 90 sec.
- The SNMPTRAP message with Enterprise OID as specified in the ACS6000-TRAP-MIB file (L3-65614727) is fixed.
- Regular users can run cli application from the shell prompt. (L3-65618098)

==========

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, 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.

Emerson and Emerson Network Power are trademarks or registered trademarks of Emerson Electric Co. Avocent, DSView and Cyclades are trademarks or registered trademarks of Avocent Corporation. All other marks are the intellectual property of their respective owners. This document may contain confidential and/or proprietary information of Avocent Corporation, and its receipt or possession does not convey any right to reproduce, disclose its contents, or to manufacture or sell anything that it may describe. Reproduction, disclosure, or use without specific authorization from Avocent Corporation is strictly prohibited. ©2012 Avocent Corporation. All rights reserved.