Avocent® Corporation
ACS 6000 Advanced Console Server
Release Notes
Version 2.4.0-11
September 2nd, 2011

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

==========

Please refer to the Installation/Administrator/User Guide for detailed instructions to update the ACS 6000 console server to version 2.4.0.

In order to have all features listed in this release available through DSView™ 3 management software, DSView™ 3 software version 3.7.1 or later and ACS 6000 console server plug-in version 2.4.0.2 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 (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 versions 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_2.4.0.11	FL0585-019.bin FL0585-019.bin.md5	FL0585-019

==========

Features/Enhancements

==========

Please refer to the Installation/Administrator/User Guide and/or Command Reference Guide for details about features supported by the ACS 6000 console server version 2.4.0.

Major feature of the ACS 6000 console sever version 2.4.0-11 include:
1. 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:

1. ACS 6000 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.
    - Customer can enable or disable the FIPS Module via OBWI or CLI. 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 of the appliance will be longer when the FIPS Module is enabled because of the power-up self test (it takes almost 10 min).
    - 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.

2. Web User Interface usability enhancements:
    - My Computer: new option to transfer 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 store file in the computer for "Save Configuration".

3. Event Notifications: new events when 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

4. Login Banner support.
    - Administrator can enable and configure the login banner via OBWI and CLI.
    - The login banner is supported by the following sessions: Telnet, SSHv2, OBWI and console.

5. Group authorization has new attribute: session idle timeout. 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)

6. 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)

7. Feature Alert Strings supports regular expression in the configuration of the string. (Available in patch release v 2.2.0-19)

8. Multiple Routing Tables feature is supported. This feature allows 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 2.4.0-11 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 control-character in the configuration of options for ts_menu in login profile configuration (L3-65640514).
- Appliance allows customer to use control character to send break to the serial port during session against the serial port, when Break Sequence is configured with a valid control character. Valid control character is string with 2 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).
- IP alias and TCP port alias of 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)
- IP alias of serial ports does not affect remote session to the appliance (ssh/telnet session against appliance). (L3 65622292)
- The Enterprise OID is the ACS 6000 family OID (Enterprises.10418.16) in the SNMPTRAP message and in the ACS6000-TRAP-MIB.asn file. (L3 65614727)
- Serial Viewer uses the SSH port configured in Security Profile. (L3 65623184)
- Log of root user in the appliance's console port will perform authentication using configured appliance authentication type. ACS 6000 allows administrator to enable fallback to local only for root user in the appliance's console port. The configuration is available in Appliance Authentication page (by default it is disabled). (L3 65627586)
- OBWI works with IE-9 and Firefox 5 clients.
- Production script reports correctly Ethernet test results.
- Saveconf and restoreconf commands have option to transfer configuration file to/from TFTP server. (L3 65630647)
- Wiz command in CLI shows default gateway configured via OBWI/CLI when the method is configured as static. (L3 65634438)
- Restoreconf command restores serial ports configuration between appliances with different number of serial ports. (L3 65634439)

Bug fixes include:

- Telnet Send Break command sends the break signal to the target device. (L3 65582372).
- In CLI, the option "-C" allows customer to execute CLI command in no-interactive mode. (L3-65589589).
- SNMP community name 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, ie, the logging configuration will be effective only if 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).
- CPU info shows the correct processor name: 440EPX.
- ACS 6000 console server supports chain of PM10/20 30A 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).
- Regular users can run cli application from the shell prompt. (L3-65618098)

==========

Known Issues

==========

This release contains the following known issues:

- DSView™ authentication type does not work when FIPS module is enabled.
- Firmware Upgrade for a PDU under 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 some minutes and click in the node again. When the status changes to 'On line', select the PDU again and click reboot (PDU requires 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 PDU Devices drill-down in the Web 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 on the next login.
- To use keys in SSH sessions, the authentication type should be configured as local.
- In 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 max value for polling interval is 20 sec.
- The paste configuration generated by list_configuration command should not have more than 80477 characters.
- The PPP configuration through OBWI and CLI in Dial-In pages is failing in the first time. This requires a re-configuration of the PPP fields.
- The PM firmware version 1.9.2 does not recognize the command 'currseg'. Chain of PDUs that has two segments/circuits should have the same version (for ex: all PM with v 1.9.2 or all PM with v 1.9.1).

- The Event # 308 – PDU Firmware Upgrade Result will not be generated when the PDU is Avocent® PM.
- The OTP Auto Refresh operation in DSView™ 3 is failing to restart the sequence number for the OTP user. Customer should log-in to the appliance using "root" user and run the following command: "opiepasswd –c <username>", and type the passphrase as asked for.