VERTIV™

Avocent® ACS8xxx Advanced Console System

Release Notes

VERSION 2.0.3, DECEMBER 22, 2017

Release Notes Section Outline

1 Update Instructions

2 Appliance Firmware Version Information

3 Local Client Requirements

4 Features and Enhancements

5 Known Issues

6 Compatibility Matrix

1 Update Instructions

These release notes refer to both the Avocent® ACS800 Advanced Console System and the Avocent ACS8000 Advanced Console System. Please refer to your installer/user guide for detailed instructions on updating the Avocent ACS Advanced Console System.

2 Appliance Firmware Version Information

Appliance/Product	Version	Filename
Avocent ACS800 Advanced Console System Avocent ACS8000 Advanced Console System	2.0.3	Firmware-acs8-2.0.3.fl

3 Local Client Requirements

Software	Version
Internet Explorer®	11
Edge	40
Firefox	57
Chrome	62
Safari	8

To access the console port with factory default settings, you need terminal emulation software running 9600 bits per second, 8 bits, 1 stop bit, no parity and no flow control.

4 Features and Enhancements

- This release adds support for a RESTful API.
- This release adds serial support for the GXT4 UPS and adds additional network support.
- Improved support for Net-Vertiv PDUs. Most parameters are supported for Vertiv™ PDUs via both serial and SNMP.
- Adds support for upgrading firmware for the Vertiv™ MPH™/MPH2™ PDUs. Upgrade can be initiated over the serial port but the ACS must be able to connect to the PDU using HTTP or HTTPS.
- This release adds support for the HTML5 Serial Viewer. This is a basic viewer that can be launched with one click. The Java based viewer will still be supported but the HTML5 viewer will be the default.
- Continues support of Vertiv SN sensors (with updated 1-wire chipset).
- Restores support for Kerberos Authentication.
- Enhances DHCP by adding support for setting hostname using DHCP option 12.
- Improves the security of the digital signature used in the firmware file.
- Adds support for a second NTP (time) server. The console system will contact both NTP servers and use the best response (lowest “stratum” level).
- There are enhancements to IPSec in this release.
    - The first enhancement is IPSec Tunnel Monitoring. This adds the capability to monitor the following IPSec tunnel characteristics: Name, Status, Remote IP Address, Lifetime, Established Time, Phase 1 Algorithm, Phase 2 Algorithm and Certificate Name.
    - The ACS supports the download and storage of multiple IPSec certificate files.
    - The ACS supports the display of a selected IPSec certificate file.
    - Certificate fallback is supported in IPSec. If the currently selected certificate fails to establish the tunnel the unit will fall back to a previous configured certificate.
    - A user is able to delete a stored certificate.
- The serial console port of the console system may be disabled. Once disabled, the console will remain disabled unless it is enabled by an administrator or the console system is reset to factory default.
    - The console system can be reset to factory default by partial booting the unit 5 times.
- A “secure” erase has been added to allow the user to erase all user data when reset to factory default. This erases all user data in both configuration partitions as well as the user partition.
- This release fixes an SNMP memory leak and incorrect reporting of the sysObjectID.
- Forces the NTP client to communicate with the NTP server when enabled or disabled.

5 Known Issues

- The NTP client will not accept an update from an NTP server using its local clock as the clock source if reported timing parameters are outside the allowed range.
- The console system uses reverse path filtering which is configured in STRICT mode which means the console system will drop packets when the receiving packet source address is not routable through that interface.
- If sensors are used in conjunction with a PDU, it is recommended to connect the sensors to the PDU before the PDU is discovered by the console system.
- When restoring a configuration that was saved as a CLI script, the restoration may take longer if PDUs are a part of the configuration.
- The Ethernet interfaces are set to Auto-Negotiation. This supports copper for 10 Mbps, 100 Mbps or 1000 Mbps based on the speed of the connection to the other end. This supports 1000 Mbps for a fiber connection.
- EAP authentication only works with Windows XP.
- A reboot is required after enabling or disabling Bonding.
- There are two parameters that control Pluggable Devices. The first is Pluggable Device Detection which is located on the left menu and on the Security Profile page. The second is Pluggable Storage Devices which is located on the Security Profile page. To enable Pluggable Storage Devices both of these parameters must be enabled.
- If a user is removed from all groups then that user will automatically inherit the access rights of the built-in USER group. For strict security, make sure the built-in, "user", group has no permissions set. Then create custom groups for any user-group permissions needed. This ensures that when a user is removed from all groups that the user does not get any added permissions from belonging to the default, "user", group.
- HTTPS sometimes does not work in Firefox. Firefox does not load the certificate or it takes a long time to load the certificate. To correct this go to the Firefox Help menu and click on “Troubleshooting Information”. On the top right of the page, click on “Refresh Firefox”. This will clean up the Firefox certificates
- The format of the sendmsg command is “sendmsg username message”.
- If the Ports-Auxiliary Ports page displays the port name of ttyM1, then the internal modem is present and can be enabled and configured. If there are no entries in the Ports-Auxiliary Port page then the internal modem is not present and this port cannot be used.

6 Compatibility Matrix

ACS8xxx Advanced Console System	Avocent® DSView™ software Plug in	DSView software
2.0.3	2.0.0.0	4.5 SP7 4.5 SP8